RFID Access Control System
System Overview Document

By: Jim Schrempp, Bob Glicksman and Mike Calyer; v2, 1/14/2020

NOTICE: Use of this document is subject to the terms of use described in the document "Terms_of_Use_License_and_Disclaimer" that is included in this release package. This document can be found at:

https://github.com/TeamPracticalProjects/MN_ACL/blob/master/Terms_of_Use_License_and_Disclaimer.pdf

TABLE OF CONTENTS.

FORWARD.

The RFID Access Control System is a very complex project. The project was driven by the need for such a system at Maker Nexus, a 501(c)3 non-profit makerspace located in Sunnyvale California. This document is intended to provide the reader with an overview of the requirements and design of the project. Complete details of the project are posted in this repository and are offered to the general public under a Creative Commons open source, non-commercial license.

Interested parties may wish to implement variants of this project that meet the unique needs of their establishment or organization. We feel that it is very important for anyone who wishes to do so to read through this overview document and become familiar with the requirements and architecture of the project. It is only through a complete understanding of the project architecture that interested parties can successfully modify this project to meet their own, specific requirements and needs.

GLOSSARY AND KEY CONCEPTS.

The following terms are used throughout this document and are defined herein.

Maker Nexus. Maker Nexus is a 501(c)3 non-profit makerspace located in Sunnyvale California. https://www.makernexus.com/

EZ Facility. EZ Facility is an on-line scheduling, management and membership system. Maker Nexus has chosen EZ Facility to fulfill its customer relationship management (CRM) needs. As such, EZ Facility is the authoritative source for all Maker Nexus member information, including current membership status, current member payment status, and member "packages". Maker Nexus uses EZ Facility "packages" to record all member training, including basic operating and safety training that is required before a member can access certain locations within Maker Nexus or use certain pieces of equipment. https://www.ezfacility.com/ If you use some system other than EZFacility, then when you see this term think: "Membership Management System".

RFID. "Radio Frequency Identification". In this context, "RFID" refers to a system that uses Mifare Classic 1K NFC cards operating at 13.56 MHz. Maker Nexus members are each issued a personalized "RFID" card that contains encrypted information that identifies the card holder in EZ Facility and contains a provision for card revocation. Classic 1K cards provide a reasonable level of security to prevent card cloning or tampering at a low per-card cost from a wide variety of sources. This project utilizes NFC technology based upon the NXP PN532 chip. This chip

supports a wide variety of RFID cards, including the latest technology Mifare Desfire EV1/EV2 cards. This approach offers a pathway to upgrade the system to a higher level of security, albeit at a significantly higher price per card.

Encryption Keys. Mifare Classic 1K cards allow two encryption keys per sector, where a "sector" is a group of 4 user-read/write 16-byte data blocks. This project uses one sector of a Classic 1K card and two secret encryption keys. "Key A" is a secret key that is required to authenticate with a Maker Nexus RFID card for reading (only) of two items of data: the member's EZ Facility unique "clientID" and a randomly assigned "MN card UID", retained in the CRM system, that is used for card revocation purposes. These items of information can only be read from an RFID card by a device that knows this secret key. The second secret key, "Key B", is required to write data to the Maker Nexus sector on the RFID card and is also required to change keys on the card and to reformat a card back to its "factory fresh" condition. Key B is only used for administrative purposes – to create new cards, update/revoke cards, and to restore a card to "factory fresh" condition.

Particle. Particle is a company that provides complete "Internet of Things" (IoT) solutions, including hardware, development software, and connectivity. This project uses Particle's "3rd generation" mesh devices; specifically, the Particle Argon. The Argon is an inexpensive yet powerful microcontroller module with built-in WiFi capability. The Argon can also act as a mesh network gateway; specifically, with the lower cost Particle Xenon modules. As of this writing, we have tested use of a Xenon/Argon mesh/WiFi configuration for our stations and they appear to work. However, our initial deployment is limited to Argon devices because Particle does not yet support redundant mesh gateways with automatic failover. Therefore, each of our Particle based stations has direct WiFi connectivity via its Argon module. https://www.particle.io/

Particle Cloud. "Particle Cloud" refers to Particle's cloud platform that provides Internet device management and integration between Particle hardware modules and the Internet connected world. This project uses basic Particle cloud connectivity to communicate with Argon-based RFID stations.

Webhook. A webhook is a real time service provided by the Particle Cloud for connecting Particle processors to the larger internet. A webhook is invoked when a Particle processor publishes a specific event via Particle.publish(), passing any parameters in a JSON package. The webhook calls out to a specified URL and interprets the JSON for any parameters to use. When a response is returned from the URL, the Particle Cloud webhook returns the data to the Particle processor, optionally formatting the response. Our system uses Particle's cloud webhook capability to communicate with EZ Facility's cloud API and with a cloud-based SQL database for real-time recording of member activities within Maker Nexus.

RFID Station. Various "stations" are located within the Maker Nexus facility where members are required to "tap in" with their RFID membership card. Each station uses the Secret Key A to read information from the Maker Nexus "sector" in the RFID card that is presented. The station then communicates with EZ Facility in order to obtain membership information that is necessary

to determine if the member has access to the location/equipment under that station's control. RFID stations are configured (by an administrator) to provide specific types of access control services. There are three general types of RFID stations in this project:

> Administration Station: There is generally only one administration station provided within Maker Nexus. This station is subject to added physical security and is the only station type that can create new RFID cards, revoke old RFID cards, reset RFID cards, and update/change Maker Nexus secret encryption keys.
>
> Check-in/out station: There are one or more of these stations at each entrance/exit to Maker Nexus. Members must tap their badge at one of these stations when they enter and leave the Maker Nexus facility. Check-in/out stations use data from EZ Facility to ensure that memberships and dues are current before a member is admitted to the facility.
>
> Location/equipment station: Various subtypes of these stations are placed within Maker Nexus to check status and log member use of locations/equipment within the Maker Nexus facility. Location/equipment stations use data from EZ facility to ensure that members have the necessary safety training "packages" for that location/equipment before the member can access the associated machine or location within Maker Nexus.

Facility Database. The "facility database" is a cloud-based SQL database (with associated php software) that keeps track (in real time) of member activity within Maker Nexus. This database keeps track of members who are inside the facility and of location/equipment for each member as they tap into areas within Maker Nexus. The facility database provides administrators and emergency response personnel with immediate and current information about member location in the event of an emergency. This database can also be used to monitor access control compliance and to produce analytical reports about equipment and location utilization. RFID stations communicate with the Facility Database through a Particle cloud webhook.

Checkin Display. A web page available within the Maker Nexus facility that shows members who are currently in the facility. It also shows an indication of which stations each member has activated while in the facility. The Checkin Display is presented on at least one monitor located at a prominent spot within the facility.

PROJECT REQUIREMENTS.

Background.

Maker Nexus is a 501(c)3 non-profit makerspace located in Sunnyvale, California. The Maker Nexus mission statement is as follows:

"Our mission is to increase the capacity of individuals in our community to make things. We believe that unleashing the innate innovation in people can make their lives better, can improve our community, and can even change the world."

Safety, security, and financial viability are key concerns of Maker Nexus. Maker Nexus has a substantial amount of industrial grade equipment, including (but not limited to):

- 3D printers
- Electronics bench (including soldering equipment, test equipment and hand tools)
- Laser cutters/engravers
- Vacuum formers
- CNC embroidery machines
- Woodshop, complete with planers, joiners, table, miter and band saws, drill press, lathes, CNC router, workbenches, and hand tools
- Metal shop (in development, as of this writing)
- Classrooms, including computers
- High speed WiFi

Safety is a primary concern. Each member must pass a class (or take an alternative operation and safety test) before they are permitted to use specific items of industrial equipment. The classes emphasize safety and the proper operation and handling of each item of equipment. The scope of safety also includes staff training, procedures, and information needed for emergency first responders.

Security is a related concern. It is important to monitor who is in the facility and who is using each equipment item at all times.

Financial viability is the remaining main concern of Maker Nexus. Several previous maker spaces have gone bankrupt due to a lack of financial scrutiny and control. Financial viability includes safety, as proper safety procedures and enforcement help to reduce insurance and liability costs. Financial viability includes security because good security procedures and enforcement mechanisms reduce financial losses due to abuse, neglect, and theft. Finally, financial viability necessitates tight financial controls, including billing and tracking of memberships, dues payment, and expenditures.

Maker Nexus, like virtually all non-profits, must maintain a tight budget that limits the number of paid staff personnel needed to operate the facility. Automation is viewed as a key element in reducing staffing requirements. Maker Nexus has selected EZ Facility as its CRM system. EZ Facility is the authoritative source for all Maker Nexus membership, membership status, billing, payment tracking, and class/test completion information.

Maker Nexus has also determined that automation can assist a limited and busy paid staff via an RFID card-based access control system. This latter system is what this project is about. Each member is issued an RFID card. The RFID card is required to check in and out of the

facility and to gain access to locations/equipment within Maker Nexus. Since EZ Facility is the singular, authoritative source for all the information needed for access control purposes, the RFID card system must query EZ Facility directly, and in real-time, for information needed to make proper access control decisions. EZ Facility has a cloud API that is suitable for this purpose. However, EZ Facility does not have an RFID card system that suits this purpose. This project provides for this latter need.

The idea behind this project is that various RFID card reader stations are placed within the Maker Nexus facility. Stations are placed at the main entrance reception desk so that members can check in and check out of the facility by tapping their membership RFID card at the station. Check in/out stations are also located at secondary entrances and exits to the facility. Check - in/out stations obviate the need to staff a reception desk and to directly monitor secondary entrances/exits. Members are only permitted into Maker Nexus if they are paid up members in good standing. Otherwise, members must contact a facility manager to resolve their membership-related issue(s).

Additional RFID card stations are located inside the facility, near specific locations (e.g. textile area) or specific pieces of industrial equipment (e.g. laser cutter) that require members to pass safety and operation classes/tests before they are permitted to use the equipment. Members gain access to locations/equipment by tapping their RFID card at the location/equipment station. Members must have the proper “package(s)” within EZ Facility in order to gain access to the associated locations/equipment. An EZ Facility “package” represents completion/passing of the relevant class(es). A member who does not have the proper package(s) in EZ Facility needed to gain access to an item of equipment or a location is rejected by the RFID card system and must contact a facility manager to resolve their credentialing issue(s).

Maker Nexus staff needs to monitor the RFID card system admit/reject decisions. Two means are provided to accomplish this end. First, each RFID card station is equipped with highly visible red and green lights that clearly indicate the station’s accept/reject decision for each card tapped. Each station also has a buzzer that provides an audible indication of accept or reject. Second, a master facility display is provided on monitors located at the entrance and at other locations within the facility. This display provides a quick overview of who has been admitted into Maker Nexus and what location/equipment each admitted member has been accepted. Staff members can use this display to quickly determine who is in the facility, where in the facility they may be, and (by omission) whether someone is in the facility or using equipment for which they do not have permission. The Facility Database drives this display and the same database may be used to generate various administrative reports, such as facility and machine utilization statistics.

Top Level Requirements.

Each member of Maker Nexus shall be issued an RFID card. The member must use their RFID card to gain access to the Maker Nexus facility and to gain access to specific items or equipment or specific locations (e.g. textile area) within the facility.

The RFID card system shall query EZ facility directly, and in real-time, in order to determine whether the cardholder is permitted into the facility and/or permitted to use specific items of equipment, depending upon the RFID card station's location and function.

Each RFID station shall light a green "admit" light and beep an "admission" sound after a card is tapped and the proper credentials for that station location are obtained (for the card holder) from EZ Facility.

Each RFID station shall light a red "reject" light and beep a "rejection" sound after a card is tapped and the proper credentials for that station location are not found (for the card holder) in EZ Facility, or if some error occurs.

The RFID card system shall log all card taps and access control decisions to a cloud-based Facility Database. The Facility Database shall utilize this information to maintain a real-time display of members admitted to and present within Maker Nexus and of locations/equipment that each member has been admitted to.

Members shall be encouraged to "tap out" when leaving Maker Nexus. These taps shall be used to update the Facility Database and the associated summary status display. It is not required that members "tap out" on individual location/equipment stations.

The Facility Database shall automatically be cleared each day after the facility has closed. This will compensate for any failures to tap out from the facility.

There shall be a manual process available to Maker Nexus staff members that allows them to "tap out" any member.

Control vs Cost and Accessibility Requirements.

The RFID card access control system shall provide a "moderate" level of security and control. The term "moderate" herein is used to indicate a need for balance between the project goals and objectives on one hand, and the cost and member usability on the other hand. Specific requirements related to "moderate" security and access control are as follows:

- Access control shall be via RFID cards that are reasonably difficult to clone. The use of bar codes or unencrypted RFID tags are not acceptable. On the other hand, RFID cards/technology must be easily available at low cost.

- Physical barriers for access control are not required and are currently deemed to be an unacceptable intrusion on member satisfaction and on safety. Powering off equipment to prevent member access after RFID system rejection is not required and is currently deemed to be undesirable from an equipment longevity perspective. However, the

desirability of powering off specific items of equipment is presently under review and this limitation may be removed for certain items of equipment at some later time.

Facility Access Control Detailed Requirements.

The RFID card access control system shall query EZ Facility, in real-time, when a member taps in at a facility entrance station. The member shall be identified to EZ Facility by the EZ Facility “clientID”, which is a unique identifier for each membership record within EZ Facility.

A member shall only be admitted to Maker Nexus if (a) their membership status is “current”, and (b) they do not owe money for dues or for other purchases, and (c) their RFID card has not been revoked. If a member is rejected for any of these reasons, admission to Maker Nexus shall be rejected and the cardholder shall be directed to see a facility administrator to clear up their account.

Each time that an RFID card is tapped at a facility entrance station, the station shall check the current check-in status with the facility database to see if the card holder is already checked into Maker Nexus. If not, the station shall consider the tap to be a check-in and shall query EZ Facility for admission information as required above. If the card holder is already checked into Maker Nexus, the tap shall be considered a check out and the facility database shall be updated accordingly.

Location/Equipment Access Control Detailed Requirements.

The RFID card access control system shall query EZ Facility, in real-time, when a member taps in at a location/equipment station. The member shall be identified to EZ Facility by the EZ Facility “clientID”, which is a unique identifier for each membership record within EZ Facility.

A member shall only be admitted to the location/equipment of the station if they have the required “package(s)” for that equipment/location. If a member is rejected on this basis, use of the associated location/equipment shall be rejected and the cardholder shall be directed to see a facility administrator to clear up their records.

If the member is admitted by the station, an indication shall appear with their information on the Checkin Display.

Access control activity - positive and negative - shall be logged to the Facility Database.

Administrative Requirements.

Maker Nexus administrative personnel shall be provided with the following capabilities:

- The capability to create and issue a valid Maker Nexus RFID card to a member.

- The capability to revoke all previous cards issued to a member whenever a new card is issued.
- The capability to reset any Maker Nexus formatted cards to a “factory fresh” condition.
- The capability to determine the owner and status of an unknown RFID card.

All information needed to produce/manipulate Maker Nexus RFID cards and EZ Facility record information shall be kept secret and shall be known only to selected Maker Nexus administrative personnel.

RFID card check in/out stations and location/equipment stations shall not have the capability to write or to alter information stored on the RFID cards; only to read information from the cards securely. Only specifically designated administration stations shall have the capability to create or modify Maker Nexus formatted RFID cards.

Only duly designated Maker Nexus administrative personnel shall be able to configure or reconfigure RFID card stations to be check in/out stations, location/equipment stations for specific location/equipment, or to perform administrative functions.

Facility Monitoring Detailed Requirements.

A Facility Database shall be provided to record successful and unsuccessful taps at all check-in and location/equipment stations. Information recorded in the facility database shall be used to determine if a tap at a facility check-in station represents a check-in or check-out; i.e. toggling this status.

The Facility Database shall drive a display (e.g. web page) that depicts all members who are currently checked-in to Maker Nexus. This display shall be updated in near real-time as check-ins and check-outs take place. This display shall also show current member check-in status for each location/equipment item within Maker Nexus. Reports of check ins shall only report members who have checked in that day. Members who fail to check out the previous day shall not be reported as checked in.

Displays that are driven from the Facility Database shall be placed near the front desk and at other locations within Maker Nexus that are visible to staff members throughout the facility.

Note: the Facility Database does not supply data used to admit or deny a member access to the facility or equipment. The data for these decisions shall be provided by EZ Facility exclusively.

Technical Failure Backup Requirements.

Procedures for facility check-in and location/machine access control shall be created that operate in the event of failure of any part of the RFID card access control system. The same

procedures shall be used if a member does not have their RFID card with them and for guests who are not current members of Maker Nexus. Manual sign-in sheets are an acceptable solution.

DESIGN OVERVIEW.

The section presents an overview of the RFID access control system project design. The overview introduces the major components of the system and the data flows between them. This overview also highlights how the system design achieves the project requirements.

Top Level Design.

The overall architecture for the system is depicted in figure 1:

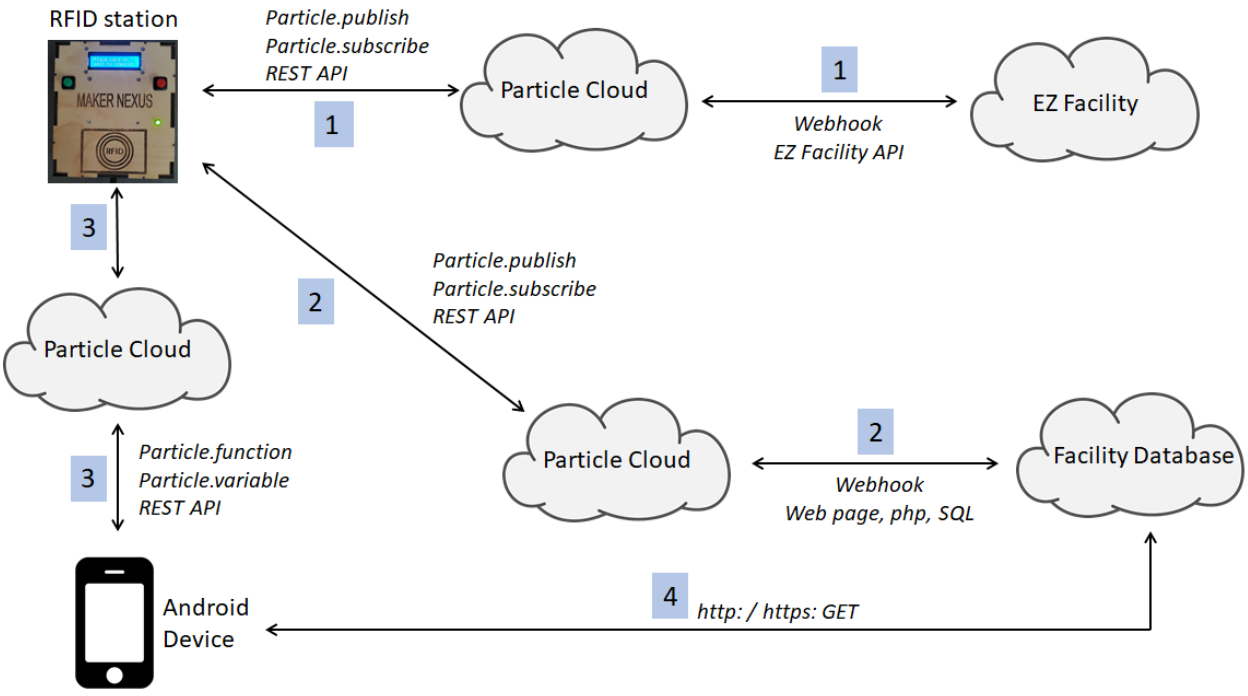

Figure 1. System Architecture.

The major components of the system are as follows:

- RFID station: There are multiple RFID stations that are part of this project. The stations are used for facility check-in, location and equipment access control, and system

administration. Each station contains a Particle[1] Argon[2]; a high-end microcontroller with WiFi – Internet access.

- Particle cloud: The Particle devices in the RFID stations communicate securely with the Particle cloud. The Particle cloud allows Particle devices to securely communicate with Internet based services via a REST interface, and also via webhooks. Both the REST interfaces and webhooks are used in this project.

- EZ Facility: EZ Facility is a cloud-based CRM system. EZ Facility offers a REST API that allows Internet connected devices to query and modify information in the EZ Facility Maker Nexus account.

- Facility Database: This is a mySQL database, with associated web pages and PHP code that is hosted in the Maker Nexus web hosting cloud account. At the moment, the database consists of a single table that is a log of all transactions recorded there by the RFID stations[3].

- Android Device: This is any WiFi-connected android smartphone or tablet. As of this writing, an inexpensive 7" Kindle Fire tablet is used, but most any Android device will do. This device hosts apps that Maker Nexus administrators can use to configure other stations, to manage RFID cards, and other related administrative functions.

The various flows of data within the system are depicted by numbers above the arrows in figure 1.

(1) Several webhooks have been created to communicate with EZ facility using the EZ Facility API. These webhooks are stored in the Maker Nexus RFID Admin account on the Particle cloud. Each webhook is triggered by a *Particle.publish()* statement in the Argon's firmware. Each Argon receives webhook responses via *Particle.subscribe()* statements. Webhooks are provided to: (a) Obtain a temporary access token (OAuth) to the Maker Nexus EZ Facility account, (b) Obtain member information from EZ Facility based upon the membership number, (c) Obtain member information from EZ Facility based upon the EZ Facility ClientID field, (d) Obtain package information for a member

[1] www.particle.io

[2] Any 3rd Generation Particle device may be used in RFID stations. The Argon provides WiFi access to the Internet directly. Xenons can be used to provide Internet access indirectly, via the Particle mesh network capability, using an Argon or Boron as the Internet gateway. We have tested a Xenon working through an Argon as the gateway but have not currently deployed any Particle devices other than Argons. As a result, each RFID station communicates directly with the Particle cloud over the Maker Nexus WiFi.

[3] Another table is used to store information about RFID station types, the codes associated with each station type, and the credentials (packages) needed for member access to locations/equipment. This table provides centralized definition and control of station types and access requirements.

from EZ Facility, and (e) check a member in to EZ Facility (check-in to Maker Nexus). (Note, this EZ Facility check in is made to enable EZ Facility reports. It is separate and distinct from the Facility Database check in logging and reporting.)

(2) Three webhooks have been created to communicate with the Facility Database via the webserver and php. The first webhook logs events from an RFID station to the Facility Database. The second webhook retrieves information from the Facility Database back to the RFID Station to determine if a member is checking in or out. The third webhook returns admission criteria and station codes for each type of RFID station defined for the facility.

(3) Apps on the Android device communicate with RFID stations to assist Maker Nexus administrators with managing the various RFID station types and with making, revoking, and verifying Maker Nexus RFID cards. Each app communicates with the Administration RFID station via WiFi-Internet to the Particle cloud. Functions on the RFID station are exposed to the Particle cloud via *Particle.function()* declarations within the firmware. Likewise, data items within the RFID Station firmware are exposed to the Particle cloud via *Particle.variable()* declarations within the firmware. Apps on the Android device call such functions and read such variables via Particle's REST interface to the Particle cloud.

(4) A REST interface (http: or https: GET) calls a php script that returns a JSON formatted list of station types and station type codes from the Facility Database. A central table in the Facility Database defines all station types, their type codes, and the criteria for admitting a member to the location corresponding to each station type.

RFID Station Design.

Figure 2 depicts the internals of an RFID station. All RFID stations contain identical hardware and firmware. The station's function is set by calling a cloud function on that station with an argument that designates the type and function of that station. The cloud function can be called from an android app or via the Particle Console.

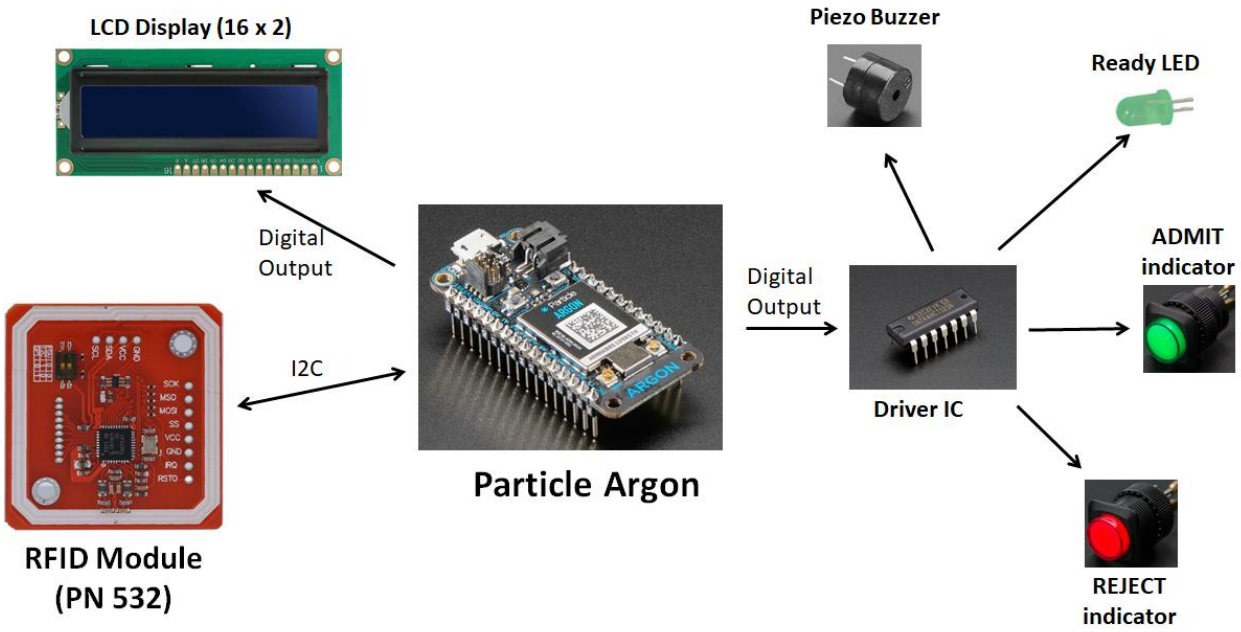

Figure 2. RFID Station Hardware.

Each RFID station contains the following major components:

- Particle Argon. The Particle Argon is the central "brain" of an RFID station. The Argon contains an advanced microcontroller and internal WiFi capability. The Argon uses WiFi to communicate with the Particle cloud. This communication allows the Argon to be re-programmed "over the air" with new firmware. It also provides for "cloud communication" between the Argon and the other components of the system. As a microcontroller, the Argon communicates with the other hardware components of the station via it's I/O ports.

- RFID module. The RFID module provides near field power and communication with RFID cards that come it close proximity to it. The module used in the RFID station uses a PN532 chip from NXP. The PN532 can communicate with a wide variety of RFID/NFC cards, including the Mifare Classic 1K cards used in this project. The RFID module offers several means of communication with a host processor. I2C communication is used in the RFID station because it is reliable, is supported by the Argon, and uses only 3 I/O pins (including an "interrupt" signal to the microcontroller).

- LCD display. A two-line, sixteen character per line LCD display is used to provide prompts and feedback between the Station and an RFID card holder. A 3.3 volt LCD module is required to interface with the Argon without additional level shifting circuitry.

- Driver IC. A 74AHCT125 driver is used to integrate LEDs and a buzzer with the Argon microcontroller. This IC allows these external devices to be powered from the Station's

5 volt power supply, thereby limiting drain on the Argon's 3.3 volt regulator. The driver IC converts 3.3 volt outputs from the Argon to 5 volts that power these external devices.

- Piezo Buzzer. A piezo buzzer is used to provide audible feedback to users and other people in the vicinity of a Station. User interactions with a Station will normally resolve into either acceptance of their use of the facility or of some equipment, or rejection of their request to use the facility or equipment. The Argon firmware produces distinctive sounds from the piezo buzzer when an accept or reject decision is made.

- Ready LED. A simple, green LED is used on the Station to inform a user that the Station is ready for them to tap their RFID card on the RFID reader.

- Admit indicator. A large, green LED indicator is used to provide visual feedback to users, and to other people in the vicinity of a Station, of acceptance of their RFID card and of their request for access to the facility or equipment (depending upon the Station type and location).

- Reject indicator. A large, red LED indicator is used to provide visual feedback to users, and to other people in the vicinity of a Station, of rejection of their RFID card or of their request for access to the facility or equipment (depending upon the Station type and location).

All of these station components are packaged into a custom enclosure that is assembled from laser cut panels. Complete CAD files for laser cutting the enclosure parts, as well as complete instructions and parts lists for assembling an RFID station are included in this repository.

Administrative Station Design.

The Administrative version of the RFID Station contains the same hardware and the same Particle firmware as all other versions of the RFID Station. In addition, the administrative version of the Station requires an Android device with an app called "MN_Card_Admin". This app provides administrators with a user interface to:

- Query the EZ Facility database for the ClientID number for a member.
- Format RFID cards for members.
- Identify the contents and format of an unknown RFID card.
- Reset an RFID card that was previously formatted for Maker Nexus to a "factory fresh" state.

The app does not communicate directly with EZ Facility. The app communicates with the administrative Station's Argon via the Particle cloud. The firmware on the Argon then communicates with EZ Facility using webhooks and *Particle.publish()* and *Particle.subscribe()* firmware commands.

The Android app(s) communicate with the Argon using Particle's REST API to the Particle cloud. The Particle cloud, in turn, communicates with the Argon using Particle's proprietary, secure internal protocols. A detailed description of the cloud functions and cloud variables involved in this interface is in the document "MN_Card_Writer_API" which is published in this repository.

RFID Station Type Selection.

An Android app called "MN_Station_Configurator" provides administrators with the ability to configure an RFID Station to be an administrative Station, a check-in Station, or any other type of Station (various flavors of location/equipment stations). All RFID Stations share the same hardware and firmware design. A Station is configured to become a certain type by using this app to select the desired type from a list of station types stored in the Facility Database. This station type list contains the station type, a type code for each type, and the criteria for accepting a member into the location/equipment associated with each station type.

The MN_Station_Configurator app makes an http: or https: GET call to a php script on the Facility database server ("*fdbGetStationConfig.php*"). The URL, including the script call, is user-configurable within the app. The script queries the Facility Database and returns a JSON formatted list of station types and their associated station codes. The user then selects the desired station type and commands the selected Station to become that type via a *Particle.function()* cloud call to the selected Particle device (selected station) ("*setDeviceType(device type code)*"). This cloud function can also be called with an argument of -1 (device types are positive numbers) after which the RFID Station returns the currently set device type to the app.

After an RFID Station to configured to be a certain type via the *setDeviceType()* cloud call from this app, the station firmware uses a webhook "*fdbGetStationConfg*" to query the Facility Database to return a JSON formatted list of member admission criteria for the selected station type.

The "code" for this webhook is contained in this repository in the software folder in the file called "webhooks.txt". PHP source code is in the Software folder of this repository.

Design for EZ Facility Access.

The Argon in an RFID Station communicates with EZ Facility using webhooks that are stored in the Particle cloud. These webhooks are only accessible to Particle devices that are claimed into the Maker Nexus administrative account. Webhook responses from EZ Facility are only returned to the Argon that published to that webhook.

The following webhooks are involved in the EZ facility interface:

- *ezfClientByMemberNumber*: queries EZ Facility for membership information based upon the Maker Nexus membership number. This interface is primarily used by the administration Station to look up member information needed to create an RFID card for a member. Member number can be found on the personal information page for each member in EZFacility. The member number can be a mix of letters and digits, and EZFacility enforces uniqueness.

- *ezfClientByClientID:* queries EZ Facility for membership information based upon the EZ Facility "ClientID" unique key. This interface is primarily used by the administration Station to look up member information needed to determine ownership and revocation status of an unknown RFID card. ClientID is not easily discerned in the EZFacility user interface.

- *ezfGetPackagesByClientID:* queries EZ Facility for the packages (training records) that are registered for a member within EZ Facility. This interface is primarily used by location/equipment RFID Stations for member access control purposes.

- *ezfCheckInClient:* checks a client into EZ Facility for entrance into Maker Nexus. EZFacility does not have the notion of "check out".

- *ezfCheckInToken:* uses Maker Nexus secret information to obtain an OAUTH2 bearer token that is subsequently used for secure access to EZ Facility in all of the other webhook API functions (above).

The "code" for these webhooks is contained in this repository in the software folder in the file called "webhooks.txt".

Design For Facility Database.

The Facility Database is a mySQL database that is used for logging events generated by the RFID stations. Each record in the database contains:

- the RFID station local time
- the Particle coreID that generated the request
- the device function
    - If the log record was made by an RFID station, this will be the function of the station at the time the request was made (Check In, Woodshop, Laser, etc)
    - If the log record was made by another source, such as a PHP script, then that name will be in the field.
- the Particle EventName (this will be the webhook name)
- the clientID
- the client's first name
- a log event name (this is the truly significant information)

- any log data

One important event is member check in and check out. EZ Facility only provides the capability to record member check-ins to Maker Nexus. The Facility Database records all Station events including facility check-ins and check-outs as well as location/equipment check-ins (access requests).

When an RFID Check-in Station posts a check-in event to the Facility Database system, the system checks to see if the user is already checked-in. If so, the system will enter a Checked Out record in the database. The system returns the action it took so that the RFID Station can inform the user if a check-in or check-out occurred.

The Argon in an RFID Station communicates with the Facility Database using webhooks that are stored in the Particle cloud. These webhooks are only accessible to Particle devices that are claimed into the Maker Nexus administrative account. Webhook responses from the Facility Database are only returned to the Argon that published to that instance of the webhook.

The following webhooks are involved in the Facility Database interface:

- *RFIDlogging*: logs an event supplied by the Argon firmware to the Facility Database. Logging data is passed to the webhook in a JSON package.

- *RFIDLogCheckInOut*: logs a check-in request for a ClientID. The Facility Database system returns a status of check-in or check-out that is passed to the RFID Station.

The “code” for these webhooks is contained in this repository in the software folder in the file called “webhooks.txt”.

The API to the Facility Database is a set of PHP scripts that run on the server hosting the Facility Database. Direct internet access to the Facility Database is disabled. There are two main PHP scripts:

- *rfidcheckin.php*: Called from the *RFIDLogCheckInOut* webhook. Logs a device “check-in allowed” event to the database. Queries the database to see if the ClientID has already checked in on this date. If not, a CheckIn record is created. If a CheckIn record exists, then a CheckOut record is created. The result of the operation is returned to the caller.

- rfidlog.php: Called from the *RFIDlogging* webhook. The event name and data are added to the database.

- *rfidhome.html*: Various reports from the database are available. These reports are all links on the rfidhome.html page.

The PHP source code that executes webhook transactions in SQL on the mySQL database is provided in the Software folder in this repository.

The Facility Database also contains a table that lists all station types configured for a facility and the station type codes and member admission criteria for each station type so defined. This table is managed by a facility administrator and is queried (only) by the station configuration app and by RFID Stations, as described in the section “RFID Station Type Selection”, above.

Security Design and Secret Information.

The security requirements for the RFID Access Control System project are satisfied using several techniques. Chief among these is the use of secret information to access key resources, such as authentication of RFID cards and access to member information in EZ Facility. This secret information includes access controls (passwords, secret numbers, and encryption keys), particularly to cloud based resources. Physical security over various aspects of the system, particularly administrative equipment, is also employed in the overall system design. It must be emphasized that the requirements dictate a moderate level of security. Hardware costs, administration costs, and member satisfaction weigh heavily into security-related design decisions.

RFID Card Security.

The RFID cards chosen are Mifare Classic 1K cards. These cards include the provision to encrypt data on the card, using 48-bit encryption keys. The key size is relatively small for modern day systems, and there are reports of these cards being hackable by other than brute force means. On the other hand, these cards are widely used as hotel room keys and for fare collection on public transit systems around the world. As such, they are widely available at very low cost and their widespread use is similar to the needs of Maker Nexus.

The primary use of RFID cards in this system is to identify and authenticate the holder of the card so that access control decisions can be made based upon the cardholder’s membership data stored in EZ Facility. The cards themselves hold data that is not particularly secret. The main security function required of these RFID cards is that they be difficult to clone (therefore, to forge). Members are expected to keep track of their RFID card and to use their card to identify and authenticate themselves (and nobody else) to the system. If a card is lost, Maker Nexus administration can issue a new card to the member in a manner that automatically revokes the old card(s).

Figure 3 depicts the layout of a Mifare Classic 1K card for use within the Maker Nexus RFID system.

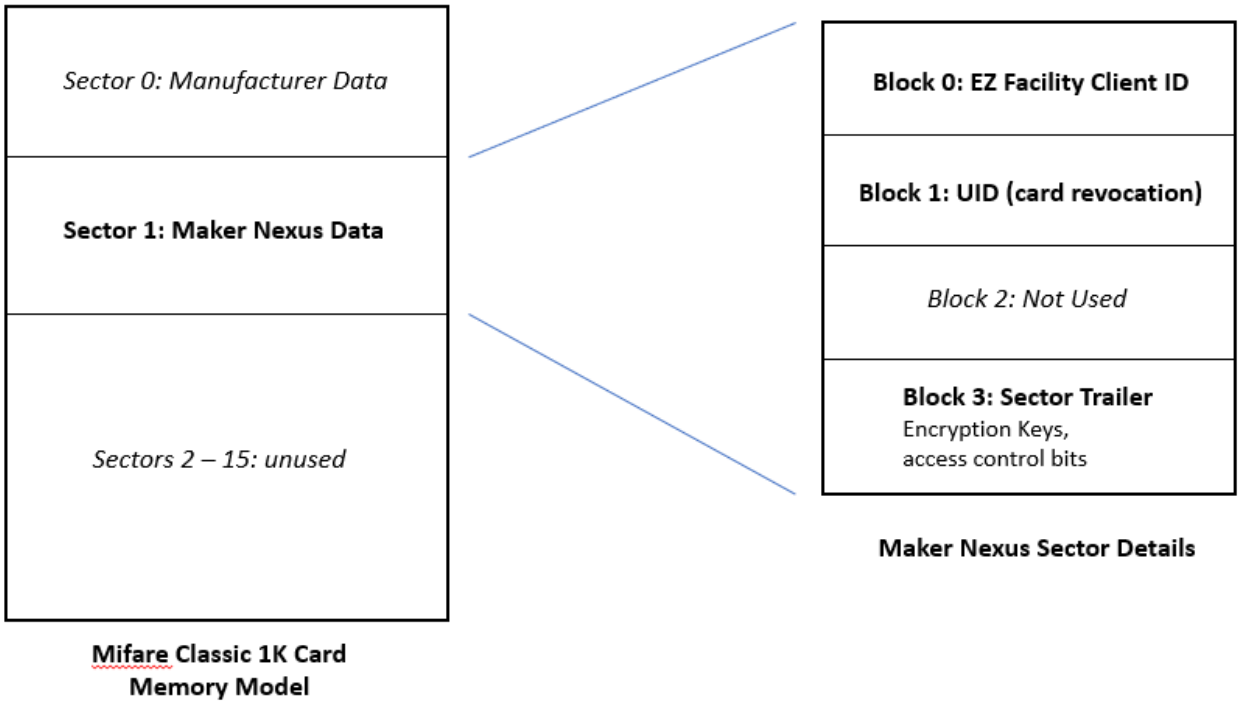

Figure 3. RFID card layout.

Classic 1K cards are divided up into "sectors". There are 16 sectors on a 1K card. Each sector contains exactly 4 "blocks" of user read/write data; 16 bytes per block. The last block in each sector is called the "sector trailer" block and this block contains two 6-byte long encryption keys (key A and key B), as well as access control bits. The access control bits define how the keys are used for read/write/modify access to each of the 4 data blocks of the sector (i.e. the three user-defined data blocks and the sector trailer block). Each of the 16 sectors has its own sector trailer block and is independent of the remaining 15 sectors on the card.

The first sector of a Classic 1K card (sector 0) contains information placed there by the manufacturer and is left alone for the purposes of this project. The Maker Nexus data is nominally stored in sector 1 of each RFID card that is issued to a member. The remaining sectors are not used by this project and may be used for any other desired purpose.

Maker Nexus maintains two secret keys for all cards issued for this project. The keys are known only to a very few people and are stored in a secure location. The keys are included in file "rfidkeys.cpp". Templates for these files, lacking the actual Maker Nexus secret keys, are included in the Software folder in this repository. These files actually contain 3 sets of keys:

- *Factory default keys*: these are the publicly known keys for all factory fresh cards. They are 0xFF (6 times) for key A and the access control bits allow key A to be used for reading and writing of all blocks inside of each sector (key B is not specified nor used).

- *Maker Nexus secret keys*: key A and key B are generated randomly and used to secure each card as it is formatted for Maker Nexus on an administration Station. Key A is used

to read (only) data from the Maker Nexus sector and cannot be used to write data nor to modify access control bits for the sector. Key B can be used for reading, writing, and modifying data on all 4 blocks of the sector.

- *Old Maker Nexus secret keys*: in the event of a security breach, it is necessary to have the current secret keys (key B, in particular) available so that the sector trailer block of existing cards can be modified to accept new keys (or to reset existing cards back to factory fresh).

RFID Stations that are configured as administrative Stations configure the trailer sector of sector 1 to contain Maker Nexus secret keys A and B, and set the sector trailer access control bits to require Maker Nexus secret key A (only) to read data from blocks 0 and 1 of this sector. The sector trailer access control bits require Maker Nexus secret key B (only) to be used to change the contents of any data block (including the sector trailer block) of the Maker Nexus sector (sector 1).

All other RFID Stations use Maker Nexus secret key A (only) to read the contents of blocks 0 and 1 (of sector 1). Block 0 data is the EZ Facility ClientID and is used to query EZ Facility for member information needed to make an access control decision for that RFID Station. Block 1 data is an arbitrary string that is stored for each member in “custom field 1” of that member’s record in EZ Facility. When a new card is created for a member, the administrator (who is creating the card) enters an arbitrary number into custom field 1 of the member’s EZ Facility record and that number is then copied to data block 1 of the Maker Nexus sector on the newly written card (the EZ facility ClientID for that membership record is written to block 0 of the Maker Nexus sector of the newly created RFID card). When a member uses their card to check-in to the Maker Nexus facility or to a location/equipment within the facility, the RFID Station firmware uses the block 0 data (ClientID) to query EZ Facility for that member’s data and it checks that the returned data from EZ facility custom field 1 matches the block 1 data on the RFID card that was presented to the RFID station. The card is accepted only if these two data items match. This feature provides the required automatic revocation mechanism. A card may contain the correct encryption keys and a valid ClientID but if the card is an old one (one that has been replaced), the custom field 1 data from EZ Facility will not match that on the card and the card will be rejected as a revoked card.

Note: In our implementation RFID cards are issued to new members using the default null string in the “custom field 1” of the user’s EZ Facility record (In the EZ Facility administrative interface this field is labeled “RFID Card UID”). If a card is lost, the administrator will enter some arbitrary string in the “RFID Card UID” field before creating a new RFID card. This will have the effect of revoking the lost card.

It is important to understand that the encryption keys used on these RFID cards are really authentication credentials. The fact that these items of data (blocks 0 and 1) are encrypted is not particularly important to the overall security architecture of this project. These data items are not, in and of themselves, particularly secret. However, these data items cannot be read

from an RFID card unless the appropriate encryption key is first used to authenticate a read or write operation on a particular sector. Therefore, security is provided in the sense that the card is unusable unless the RFID card Station can first authenticate the Maker Nexus sector (sector 1) with Maker Nexus secret key A. Furthermore, Maker Nexus secret key B is required to write data to any block in the Maker Nexus sector on these cards, as well as to change keys and access control bits for the Maker Nexus sector on these RFID cards. Therefore, these cards cannot be cloned or hacked unless the hacker knows the Maker Nexus secret keys. These secret keys are only stored in a special header file that is maintained only within the Maker Nexus production firmware build environment and which is accessible only by a few trusted Maker Nexus administrator/developers.

Note that the hardware design of the Classic 1K cards does not allow keys stored in the sector trailer block to be read, even by a bearer of the currently valid secret keys. If the secret keys are lost, the Maker Nexus sector on these cards become forever unusable.

It is always possible that a Maker Nexus secret key may be compromised. In this event, both secret keys will be changed. The header file that contains the new secret keys also contains the old secret keys, since the old keys (key B, in any event) are needed to change the Maker Nexus sector trailer block keys and access control bits to the new keys. In this manner, all currently issued RFID membership cards can be updated to use the new Maker Nexus keys.

The security features of the RFID cards described above also mean that a revoked card will need to authenticate with an RFID administration station using Maker Nexus secret key B in order to restore the card to a factory fresh state. An administration function is provided to do this, using the “factory fresh” default keys that are also stored on the secret key header file. A card can be reclaimed from a terminated member or from a revoked status by reverting the Maker Nexus sector on the card to its factory fresh state. This allows cards to be recycled and re-issued as if they were fresh “out of the box”, saving the cost of new factory fresh cards.

Station Security.

RFID Stations are mounted at various location throughout the Maker Nexus facility and are not physically secured from access by other than authorized personnel. However, the locations where these Stations are located a public and any tampering of a Station is, necessarily, a public event.

The use of Particle devices as the “brains” of each RFID Station provides a high degree of protection over software (firmware) tampering. There are only to ways to change the firmware on a Particle device: “flashing” the firmware over the Internet directly from the Particle cloud, or using “DFU mode” to flash firmware to the device over the device’s USB cable. Both of these methods require a secret OAUTH2 user access token and a Particle device ID to be presented to the device in order to flash new firmware to it. These two data items are long hex strings and are securely stored in the device owner’s account on the Particle cloud. Maker Nexus has an RFID administrative account on the Particle cloud that is used to “own” all RFID Station Particle

devices and only people who know this account's username and password can access the information/resources necessary to change a Station's firmware. Two factor authentication is available from Particle for added security.

Firmware development and testing is performed on a separate "sandbox" clone of the entire Maker Nexus RFID system and on Particle devices that are owned by the developer(s) and are not part of the Maker Nexus deployed RFID Stations. After release to production is authorized, the new firmware is transferred to the production system by a select developer/administrator who has access to the production Particle account.

Cloud Security.

Maker Nexus cloud functions are maintained in an account that is accessible only to specifically designated administrator/developers. Access to this file requires knowledge of the secret password established for this account. Two factor authentication of administrator/developers is available and can be enabled for added security.

An open development environment has been created so that various firmware and cloud software developers can develop, test and maintain software for this project. A release-to-production procedure is in place to review new software and approve it for release. Release to the production system is then made by transferring the new software to the secret production account by an authorized administrator/developer, and building the system there using the real (production) secret keys.

Secret information that is needed to access EZ Facility via the REST API is contained within the webhooks located in the Maker Nexus Particle account. The same is true for access to the facility database. Only authorized administrator/developers have the secret password needed to access this account. Likewise, two factor authentication is available for added security. The RFID stations themselves do not contain the secret information needed to access either EZ Facility or the facility database.

Administrative Security.

All RFID Stations utilize the same hardware and firmware. This minimizes cost and logistics. A generic RFID Station is made into an administrative station via a cloud function call from the Maker Nexus Particle account, or via an App that has been created for this purpose. This account is only accessible to specifically designated authorized administrator/developers. Once a Station has been configured to be an administrative Station, the Station is physically secured (lock and key) so that only designated facility administrators can use it. Only administrative Stations have the capability to issue new cards, revoke old cards and reset cards to factory fresh condition. All other RFID Stations can only read cards and make access control decisions based upon data from EZ Facility, and EZ Facility data can only be obtained via webhooks that are only available to Particle devices that are registered to the Maker Nexus Particle

administrative account. In general, there will be only one administrative Station, but the system design allows for multiple administrative Stations if there is a reason to have more than one such station.

Cost Effective Design.

Cost effectiveness is achieved through common hardware and firmware for all RFID stations. The hardware is based upon low cost Particle IoT devices. Very low cost character displays and RFID breakout boards have also been tested and documented in the parts list. Likewise, a low cost printed circuit board vendor has been identified and tested for the PCBs used to assemble station electronics.

Maker Nexus personnel have assembled enough generic RFID stations to meet the facility requirements for administration, check-in and location/equipment Stations, plus a few spares. Software developers purchase their own station hardware for development use. The deployed RFID Stations are configured by an administrator and the spare Stations are left generic so that a failed Station can easily and quickly be replaced by any available spare.

The choice of Classic 1K RFID cards for this project has already been cited as a compromise between security and cost. The cards are reasonably secure (when used as designed) and can be purchased for less than $0.30 a piece in low quantities (100 pcs) from multiple vendors on the Internet.

The need for additional user interface capabilities by administrators has been satisfied by an App for an Android device. Maker Nexus has purchased an Amazon 7” Kindle Fire tablet on a Black Friday sale for $30. An old Android phone will do as well. The App should run on just about any version of Android 2.5 or above.

CONCEPTS FOR PROJECT USE BY OTHER THAN MAKER NEXUS.

Some readers of this document intend to use this project as the basis of an RFID access control system for their own facility or organization. This section offers some guidance for various scenarios.

Implement this project in a non-Maker Nexus Facility that uses EZ Facility.

An organization that uses EZ Facility as its CRM system can adopt this project to their needs relatively easily. The Maker Nexus facility check-in process tests membership status and

member payment information from EZ Facility to make the check-in access control decision. The card revocation feature also uses custom field 1 of each member's EZ facility record to hold a number that represents the current member's card. The Maker Nexus location/equipment check-in process retrieves package information for the member and tests that the member has a package(s) that permits them to access some location or item of equipment. The acceptable packages for each type of station are contained in a table in the Facility Database, so the relationship between packages and location/equipment access is configurable without code changes.

An organization that uses EZ Facility as its CRM system but requires different facility check-in rules than Maker Nexus uses will need to change the firmware accordingly. Additionally, the webhook for *ezfClientByClientID* may need to be changed if the Maker Nexus filtering rules don't pass the necessary data through the webhook response back to the Argon firmware. Similarly, an organization that uses different location/equipment check-in rules than Maker Nexus may need to change the webhook for *ezfGetPackagesByClientID* if different filtering rules are needed to pass the webhook response back to the firmware. Note too that Maker Nexus names the packages in such a way as to make firmware testing for the necessary member package(s) easy. This part of the firmware should be studied carefully in order to determine how to accommodate different location/equipment access control rules. See the firmware functions: *isClientOkToCheckIn()* and *isClientOkForWoodshop()* for two examples.

Implement this project in a non-Maker Nexus Facility that uses a different CRM system than EZ Facility.

EZ Facility is not a general purpose relational database management system and the REST API is very specific to the EZ Facility schema. An organization that uses a different CRM system will have to change both the webhooks and the Argon firmware test rules in order to use this project in their facility. Alternatively, an organization may implement the relevant parts of their CRM system in a general purpose relational database management system. In this event, it might be possible to emulate the relevant EZ Facility API calls on such a system (e.g. via PHP/SQL) so that the webhooks and firmware can be used without any changes.

In general, all code that interfaces the CRM to the system can be found in firmware functions that begin with the letters *ezf.* Changing these functions and the webhooks will be needed.

Implement this project in a non-Maker Nexus Facility that does not have an electronic CRM system.

An organization that does not have an electronic CRM system (and does not wish to have one) could emulate the relevant EZ Facility API calls on a general purpose relational DBMS (e.g. via PHP/SQL). Since the facility database is such a DBMS, the same DBMS can be used to store

tables containing membership status, membership dues and/or member “packages”. In so doing, the webhooks and firmware might be usable intact. Of course, an administrative front end would need to be developed to store and maintain the membership/package information in this database.