RFID Access Control System

System Overview Document

By: Jim Schrempp, Bob Glicksman and Mike Calyer; draft 11/21/2019

**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

A close up of a sign

Description automatically generated

© 2019/2020 Team Practical Projects, Maker Nexus, Bob Glicksman, Jim Schrempp and Mike Calyer. All rights reserved.

# 

# 

# 

# TABLE OF CONTENTS.

[**TABLE OF CONTENTS**. 1](#_Toc25226890)

[FORWARD. 2](#_Toc25226891)

[GLOSSARY AND KEY CONCEPTS. 2](#_Toc25226892)

[PROJECT REQUIREMENTS. 4](#_Toc25226893)

[Background. 4](#_Toc25226894)

[Top Level Requirements. 6](#_Toc25226895)

[Control vs Cost and Accessibility Requirements. 7](#_Toc25226896)

[Facility Access Control Detailed Requirements. 7](#_Toc25226897)

[Location/Equipment Access Control Detailed Requirements. 8](#_Toc25226898)

[Administrative Requirements. 8](#_Toc25226899)

[Facility Monitoring Detailed Requirements. 9](#_Toc25226900)

[Technical Failure Backup Requirements. 9](#_Toc25226901)

[DESIGN OVERVIEW. 9](#_Toc25226902)

[Top Level Design. 9](#_Toc25226903)

[RFID Station Design. 12](#_Toc25226904)

[Administrative Station Design. 13](#_Toc25226905)

[Design for EZ Facility Access. 14](#_Toc25226906)

[Cloud Based Database Design. 15](#_Toc25226907)

[Security Design and Secret Information. 15](#_Toc25226908)

[CONCEPTS FOR PROJECT USE BY OTHER THAN MAKER NEXUS. 15](#_Toc25226909)

[Implement this project in a non-Maker nexus Facility that uses EZ Facility. 16](#_Toc25226910)

[Implement this project in a non-Maker Nexus Facility that uses a different CRM system than EZ Facility. 16](#_Toc25226911)

[Implement this project in a non-Maker Nexus Facility that does not have an electronic CRM system. 16](#_Toc25226912)

# 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 an 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 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 use certain pieces of equipment. <https://www.ezfacility.com/>

**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 to 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 membership RFID card for reading (only) of two items of data: the member’s EZ Facility “clientID” and a randomly assigned “MN card UID” 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 connectivity 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. It also uses Particle’s cloud “webhook” integration 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 reads 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 are 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 of these stations are placed within Maker Nexus to status and log member use of equipment/locations 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 in and out of 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.

# 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 the front 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. each laser cutter) that require members to pass safety and operation classes/tests before they are permitted to use the equipment. Members gain access to equipment/locations 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 equipment/location. 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. A 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.

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 equipment/locations that each member has been admitted to.

Members shall be encouraged to “tap out” from each location/equipment that they previously tapped in to when they are through using that location/equipment. These taps shall be used update the facility database and the associated summary status display. Likewise, members shall be encouraged to “tap out” when leaving Maker Nexus. These taps shall be used update the facility database and the associated summary status display.

The facility database shall automatically be cleared each day after the facility has closed. This will compensate for any failures to tap out from a location/equipment or from the facility overall.

## 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 “packages” 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.

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

## 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 equipment/location 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 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 station represents a check-in or check-out; i.e. toggling this status.

The facility database shall automatically check-out all remaining check-ins within the database after the Maker Nexus facility has closed for the day.

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 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.

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 make check-in decisions. The data for check-in 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:

A close up of a map

Description automatically generated

*Figure 1. System Architecture.*

The major components of the system are as follows:

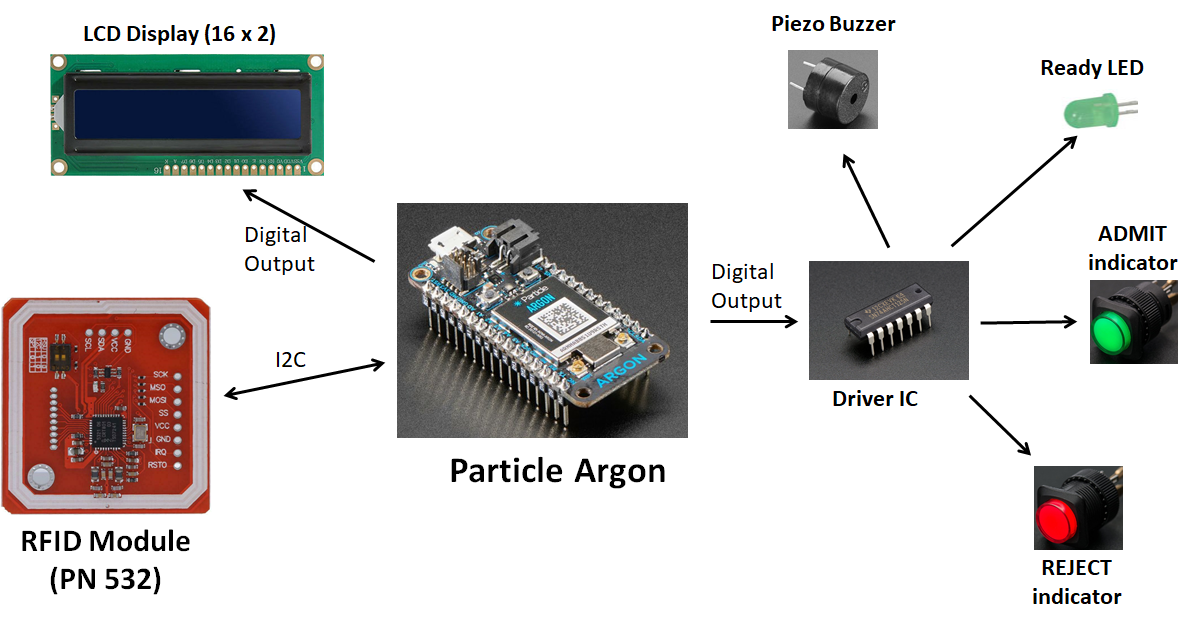
* RFID station: There are multiple RFID stations that are part of this project. The stations are used for facility check-in, location and equipment access control, and system administration. Each station contains a Particle[[1]](#footnote-1) Argon[[2]](#footnote-2); a high-end microcontroller with WiFi – 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-based 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.
* Android Device: This is any WiFi-connected android smartphone or tablet. As of this writing, an inexpensive 7” Kindle Fire table is used, but most any Android device will do. This device hosts apps that Maker nexus administrators can use in conjunction with the administration version of the RFID station 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 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 from a member from EZ Facility, and (e) check a member in to EZ Facility (check-in to Maker Nexus).
2. Two 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.
3. App(s) on the Android device communicate with an Administration version of the RFID station to assist Maker Nexus administrators with managing the various RFID station types and with making, revoking, and statusing 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.

## RFID Station Design.

Figure 2 depicts the internals of an RFID station. All RFID stations contain identical hardware and firmware. The station 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 a 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 4 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 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 acceptance of their RFID card and 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.

## 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.
* *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 unknow RFID card.
* *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.
* *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”.

## Cloud Based Database Design.

The Facility Database is a mySQL database that is used for logging member check in and check out events. 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) and check-outs. The Facility Database thus provides additional administrative and access control information. The Facility Database also provides check-in and check-out status for a member at the facility or at some location/equipment. This information is used by RFID station firmware to determine if a card tap is for checking in or checking out from that station.

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 webhook.

The following webhooks are involved in the Facility database interface:

* *RFIDlogging*: logs an event supplied by the Argon firmware to the Facility database.
* *RFIDLogCheckInOut*: requests the current check-in or check-out data for a member from the Facility Database. Used to determine if an RFID card tap at a station is a request for access (check in) or a check out from that station’s location.

The “code” for these webhooks is contained in this repository in the software folder in the file called “webhooks.txt”. The PHP source code that executes webhook transactions in SQL on the mySQL database is provided in the software folder in this repository.

## Security Design and Secret Information.

\*\*\*LEFT OFF HERE\*\*\*\*

# CONCEPTS FOR PROJECT USE BY OTHER THAN MAKER NEXUS.

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

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

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

1. [www.particle.io](http://www.particle.io) [↑](#footnote-ref-1)
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. [↑](#footnote-ref-2)