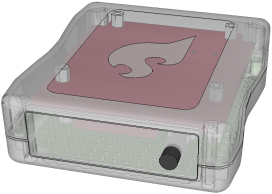
125kHz RFID Reader

User Manual



CE

Version: April 21, 2014

Steve R. Gunn
Electronics and Computer Science
University of Southampton

Contents

1 Overview

The RFID reader operates on the principle of inductive coupling to read the information from a tag or card. The tag is a passive device which powers itself from the 125kHz electromagnetic field of the reader. The field is strong enough to read a tag up to around 5cm from the reader. The tag's identity is stored as a 32-bit identifier. In total the tag transmits 64-bits which also contain a header, an 8-bit version number, parity check bits and a stop bit. These bits are Manchester encoded and communication is achieved by amplitude modulation of the 125kHz from the reader by the tag. There are two main standards for RFID communication frequencies, the other being at 13.56MHz which is used by the majority of bank cards; these systems are not interoperable.

The unit is pictured in figure 1 and is equipped with a power switch, a mode switch and a 16×2 line LCD. On

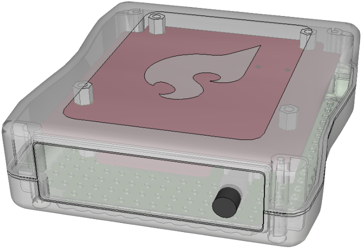


FIGURE 1: 125kHz RFID reader

power-up the system enters a scanning mode where the ID of a tag can be read and displayed on the LCD. Other modes can be selected by pressing the mode switch and full details are given in section 2. The unit operates from 2×AAA batteries which should provide a continuous operating time of around 10 hours.

2 Operation

The unit operates in one of five modes:

Scanning The tag data can be read and displayed on the built-in LCD.

Spoof The reader can emulate a tag and if placed in the vicinity of a second reader will activate it.

Signal Strength The display will show the quality of the tag signal.

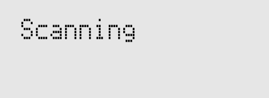
System Health The battery level and temperature status are displayed.

Diagnostic Mode Provides a mechanism for inspecting the captured sample buffer.

The operation of the modes are now described in detail.

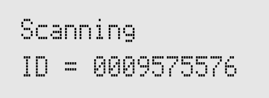
2.1 Scanning

At power on the device will enter the scanning mode. In the scanning mode the reader will repeatedly scan for a new tag. During scanning for the first tag after power-on the following message is displayed.



```
Scanning
```

If a tag is found, the data is analysed, the result displayed on the LCD and a sound is emitted to indicate that tag data was read. On placing a tag successfully in the vicinity of the reader, the tag's ID should be displayed.



```
Scanning
ID = 0009575576
```

If the reader detects a signal but is unsuccessful in decoding the ID, it will display a 16-bit error code in hexadecimal notation (see section A for further details). The first bit corresponds to whether the header was found, and if this cannot be found the following message will be displayed.

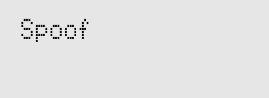
```
Scanning
Error Code 8000
```

If the header is found but some of the parity checks failed, then a message similar to the following will be displayed.

```
Scanning
Error Code 7A6E
```

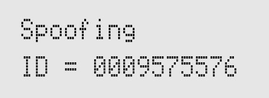
2.2 Spoofing

In this mode it is possible to get the reader to emulate a tag. First a known tag which is to be spoofed must be presented to the reader. During this phase of scanning for the ID the reader will display



```
Spoof
```

If the reader successfully reads the tag it will switch to spoof mode and the display will change to

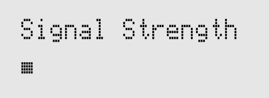


```
Spoofing
ID = 0009575576
```

If the reader is unsuccessful it will display the relevant error code and continue scanning for a valid ID.

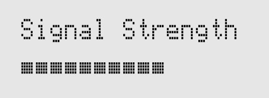
2.3 Signal Strength

The unit includes a signal strength meter which displays the strength of amplitude modulation of any tag placed in its vicinity. When no modulation is present the following display is shown.



```
Signal Strength
▦
```

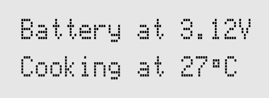
When a good signal is detected the display will change.



```
Signal Strength
▦▦▦▦▦▦▦▦▦▦
```

2.4 System Health

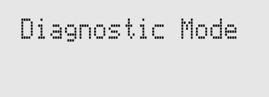
The battery voltage and the internal temperature of the microcontroller can be displayed. This information is updated twice a second.



```
Battery at 3.12V
Cooking at 27°C
```

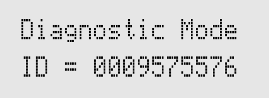
2.5 Diagnostic Mode

This mode enables the internal sample buffer of the unit to be transmitted over a serial connection for analysis. The data is transmitted in 8N1 at 19200 baud over the MISO output pin inside the unit. Whilst waiting for data the following message is displayed.



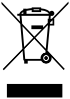
```
Diagnostic Mode
```

On discovering a tag the sample buffer is transmitted and the display is updated.



```
Diagnostic Mode
ID = 0009575576
```

3 Environment



A Error Codes

Bit	Description
15	Header not found
14	Parity error (row 0)
13	Parity error (row 1)
12	Parity error (row 2)
11	Parity error (row 3)
10	Parity error (row 4)
9	Parity error (row 5)
8	Parity error (row 6)
7	Parity error (row 7)
6	Parity error (row 8)
5	Parity error (row 9)
4	Parity error (col 0)
3	Parity error (col 1)
2	Parity error (col 2)
1	Parity error (col 3)
0	Stop bit error

Notes