Si4010 Key Fob AES Demo Kit with EZRadio® LCD Base Board User's Guide

1. Purpose

This user's guide describes the use of the Demo Kit and gives the user a brief introduction to the AES encryption/decryption algorithm. The current version of the firmware does not support remote mode, so it can only be used in standalone mode without the Wireless Development Suite (WDS).

2. Kit Contents

The kit contains the following items:

Qty	Part Number	Description
1	4010-KFOB-xxx	Si4010 universal key fob for 316.66/433.92/868.3/917 MHz
1	MSC-LCDBB930-AES	LCD Base Board with C8051F930 MCU
1	4355-PRXBxxxB	RF Pico Board with EZRadio chip for 316.66/433.92/868.3/917 MHz
1	MSC-AT50-xxx	Antenna for 316.66/433.92/868.3/917 MHz
1	MSC-PLPB_1/2/3	Key fob plastic case
1	CR2032	CR2032 Coin Cell battery
3	AA	1.5 V AA battery
1	USB	USB mini-B cable

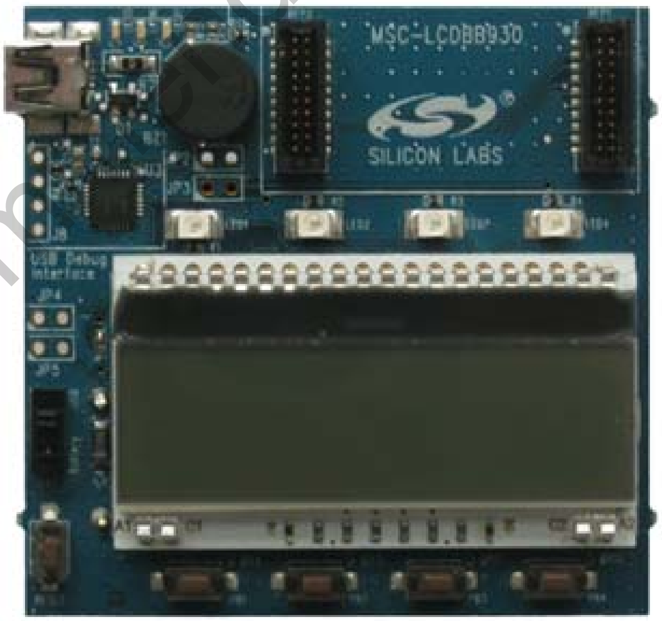


Figure 1. LCD Base Board

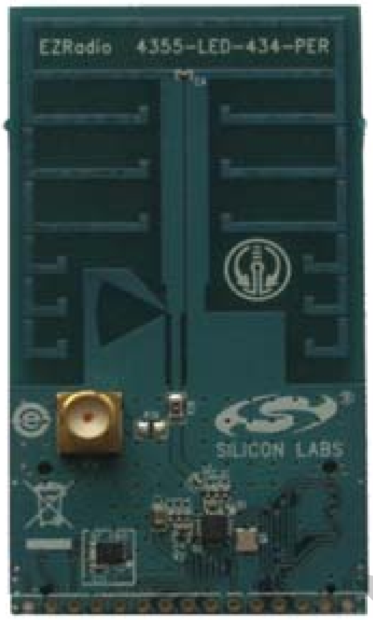


Figure 2. RF Pico Board

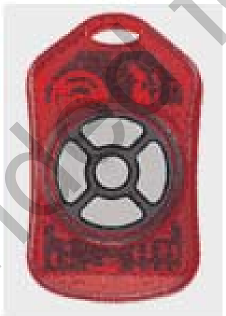


Figure 3. Si4010 Key Fob

3. Requirements

The following items are required to use the demo in standalone mode:

- LCD Base Board
- RF Pico Board with EZRadio Next Generation chip
- 3xAA batteries or USB Mini-B cable
- Si4010 key fob on 316.66/433.9/868.30/917.00 MHz

4. Si4010 Key Fob Demo Description

The AES demo utilizes the capabilities of the Si4010 key fob transmitter and the Si4355 EZRadio receiver in order to demonstrate a one-way secure link application.

The Si4010 key fob as the transmitter sends radio packets with partially encoded content. At the receiver side an EZRadio receiver, the Si4355 chip receives the packet, then evaluates and decodes it.

The receiver can handle OOK or 2FSK modulated RF packets as well as the transmitter can set up to transmit OOK or 2FSK modulated RF packets.

4.1. RF Parameters

The Si4010 AES Demo transmitter and receiver uses the following RF configuration:

- Center frequencies: 316.66/433.92/868.3/917 MHz depending on RF Pico board and key fob
- OOK/2FSK modulation (selectable)
- 9.6 kBaud
- Manchester coding in OOK mode (results in 4.8 kbps data rate).

4.2. Selection of Si4010 Key Fob Modulation

The Si4010 key fob can modulate RF packets in OOK/2FSK. In order to select the appropriate modulation type, follow the steps below:

1. Open the plastic case of the key fob.
2. Remove the battery and wait for 30 seconds to discharge capacitors.
3. For 2FSK modulation, place the battery back and make sure that no buttons are pressed during battery insertion.
4. For OOK modulation, press and hold the center button on the key fob during the battery insertion process.
5. Fit the plastic case of the key fob.

4.3. RF Packet Formats

The packet format sent by the Si4010 is as follows:

Table 1. RF Packet Format

Preamble	Sync	Chip ID	Status	Counter	CRC	AES part	CRC
13 byte	2 byte	4 byte	1 byte	2 byte	2 byte	16 byte	2 byte

The fields other than AES part are not encoded. The AES encoded part of the RF packet contains the following encoded fields:

Table 2. AES Encoded Fields

Temperature	Battery Status	Rolling Counter	Button State	PACap value	Chip ID	Reserved (0x00)
2 byte	1 byte	4 byte	1 byte	2 byte	4 byte	2 byte

Since the plain part and the AES encrypted part both contains the Chip ID, the decoding process is verified by comparing the Chip ID field between the two parts of the RF packet. If the decryption fails, a notification screen appears describing the AES decryption failure.

4.4. AES Encoding

The AES encryption/decryption algorithm is a symmetric algorithm because the same key is used for encryption and decryption. The AES128 encoding/decoding process has been done using the SiLabs AES128 library. A session key for each packet is generated based on the sender Chip ID field and the constant key for the given packet type. There are two kinds of RF packets the key fob can send: an Association packet or a Message packet. There are different keys stored in the flash for each kind of packet. The receiver determines which key should be used by the Association flag in the plain Status byte.

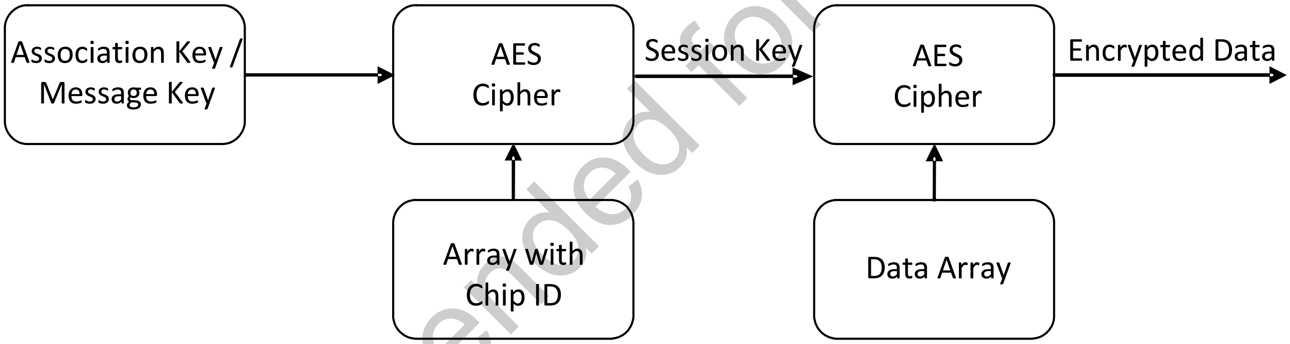


Figure 4. AES Encoding

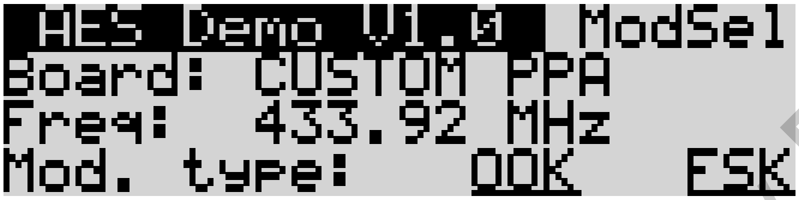
Decoding of AES encrypted data basically consists of the same steps as encoding except that the final AES cipher is replaced with inverse-ciphering. The receiver generates the same session key from the constant key and the sender Chip ID, and, since the AES is a symmetric algorithm, it can decrypt the data if the session key is valid.

5. Demo Usage

Connect an appropriate RF Pico board to the LCD Base Board; then, set the SW1 switch on the LCD Base Board according to the power source (battery or USB).

During startup, the RF parameters are automatically detected by the demo software based on the EBID information. In this way, only the modulation type (OOK/FSK) should be selected manually.

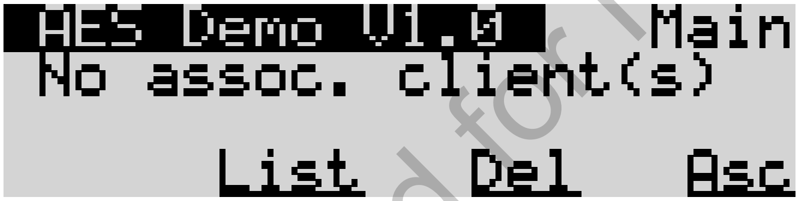
Figure 5 shows the modulation selection screen.



```
AES Demo V1.0  ModSel
Board: CUSTOM PPA
Freq:  433.92 MHz
Mod. type:   OOK   FSK
```

Figure 5. Modulation Type Selection

To select the modulation type on the Si4010 key fob, refer to "4.2. Selection of Si4010 Key Fob Modulation" on page 3. After the modulation has been chosen, the AES Demo main screen will display as shown in Figure 6.



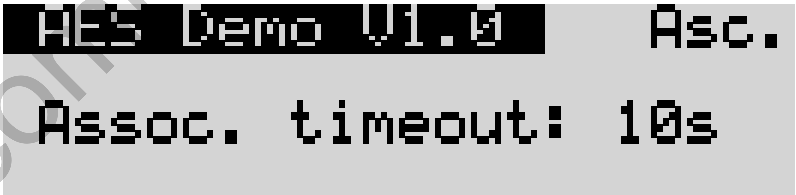
```
AES Demo V1.0    Main
 No assoc. client(s)

      List   Del   Asc
```

Figure 6. Main Screen

Notification screens discussed below can pop up in the Main screen view and are caused by various events. The notification screens disappear after a time-out of several seconds; they can also be eliminated by pressing any of the push buttons.

After startup, no associated clients are registered. In order to associate a client, press the push-button under the Asc menu option. During association, there is a limited amount of time available to associate a client. The remaining time is written to the screen as shown in Figure 7.



```
AES Demo V1.0    Asc.

 Assoc. timeout: 10s
```

Figure 7. Association Timeout

The radio packets sent by the key fob are not like the association packets sent during normal use. To get an association packet out from the key fob, press Button 1 and Button 3 at the same time. This causes the key fob to generate an association plain text packet and then encrypt it with a different (association) AES key. Button 1 (right) and Button 3 (left) on the key fob are identified by arrows in Figure 8.

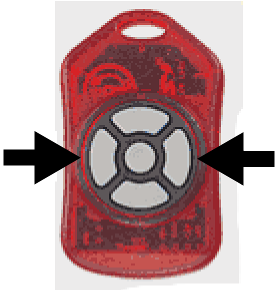
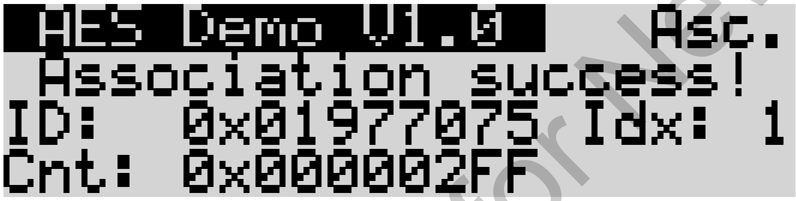


Figure 8. Key Fob Association

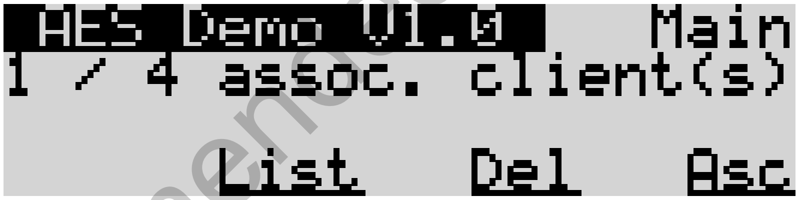
If the association timeout has not elapsed and an association request packet is received by the radio chip, the encoded part of the packet will be decrypted using an Association Session Key based on an Association Key and the sender ID. If decryption was successful, the client rolling counter is synchronized and registered to the clients list. Figure 9 shows the case when a successful association process completed.



```
AES Demo V1.0    Asc.
 Association success!
ID:  0x01977075 Idx: 1
Cnt: 0x000002FF
```

Figure 9. Association Success

When at least one client is associated, the Main screen displays the space used on the list as shown in Figure 10.



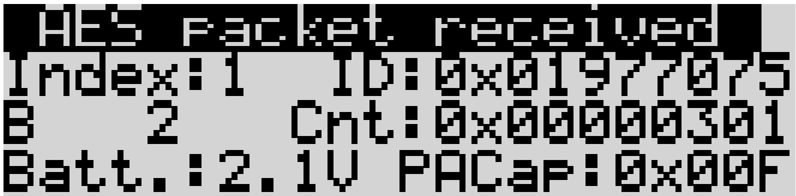
```
AES Demo V1.0    Main
1 / 4 assoc. client(s)

      List   Del   Asc
```

Figure 10. Main Screen with Associated Clients

If an AES encoded radio packet is received by the RF Pico board from an associated client (other than an association request), the payload data is decrypted and displayed on the screen. The associated clients can also send unencrypted packets, which do not need to be decrypted. The notification screen will be the same in both cases, except the title, which shows if the packet was AES encrypted or is a Plain text packet.

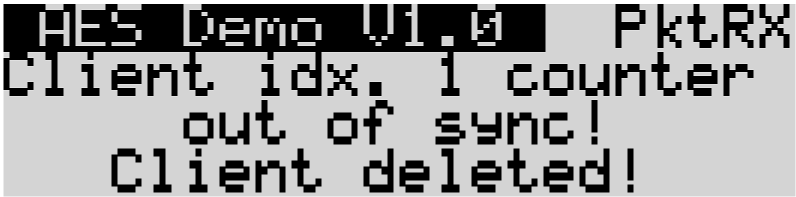
The encrypted data contains the index from the list and the ID of the sender, the button number pressed on the key fob, the rolling counter value, the key fob battery voltage, and, finally, the PACap value as shown in Figure 11.



```
 AES packet received
Index:1   ID:0x01977075
B   2   Cnt:0x00000301
Batt.:2.1V PACap:0x00F
```

Figure 11. AES Encoded Packet Received

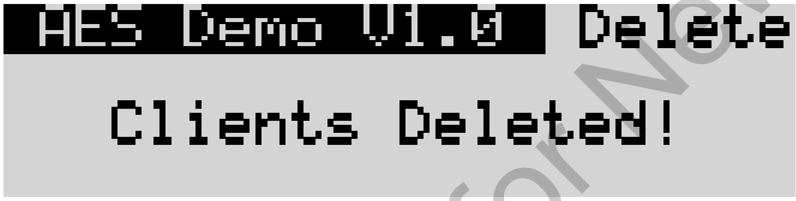
If an incoming packet rolling counter is greater than the last given rolling client counter value stored in the base Board RAM by the predefined limit, the client will be removed from the registered list, and a notification screen will be displayed as shown in Figure 12.



```
AES Demo V1.0  PktRX
Client idx. 1 counter
  out of sync!
 Client deleted!
```

Figure 12. Rolling Counter Out of Limit

The list containing the associated clients can be erased by pressing the button under the Del menu option on the Main screen. Deleting clients also resets their rolling counters. After a client is removed from the list, its packet is neither received by the Base Board nor decrypted unless it is associated again. The Delete screen is shown in Figure 13.

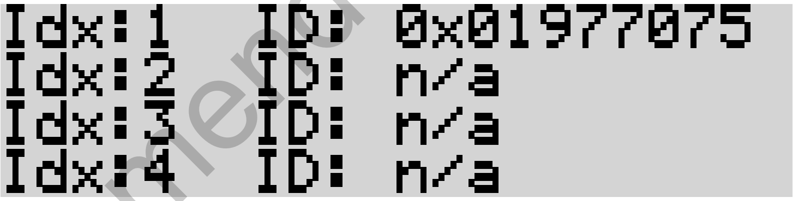


```
AES Demo V1.0 Delete

 Clients Deleted!
```

Figure 13. Delete Clients

The associated client list can be viewed by pressing the button under the List menu option on the Main screen. The list view contains the indices and chip IDs of each associated client from the list. The list view is shown in Figure 14.



```
Idx:1  ID: 0x01977075
Idx:2  ID: n/a
Idx:3  ID: n/a
Idx:4  ID: n/a
```

Figure 14. List View of Clients

6. Schematics

This section contains schematics of the RFPico, LCD Base Board, and Si4010 key fob boards included in the kit.

High-definition schematics and a complete manufacturing pack with CAD/CAM files and BOMs can be found at www.silabs.com.

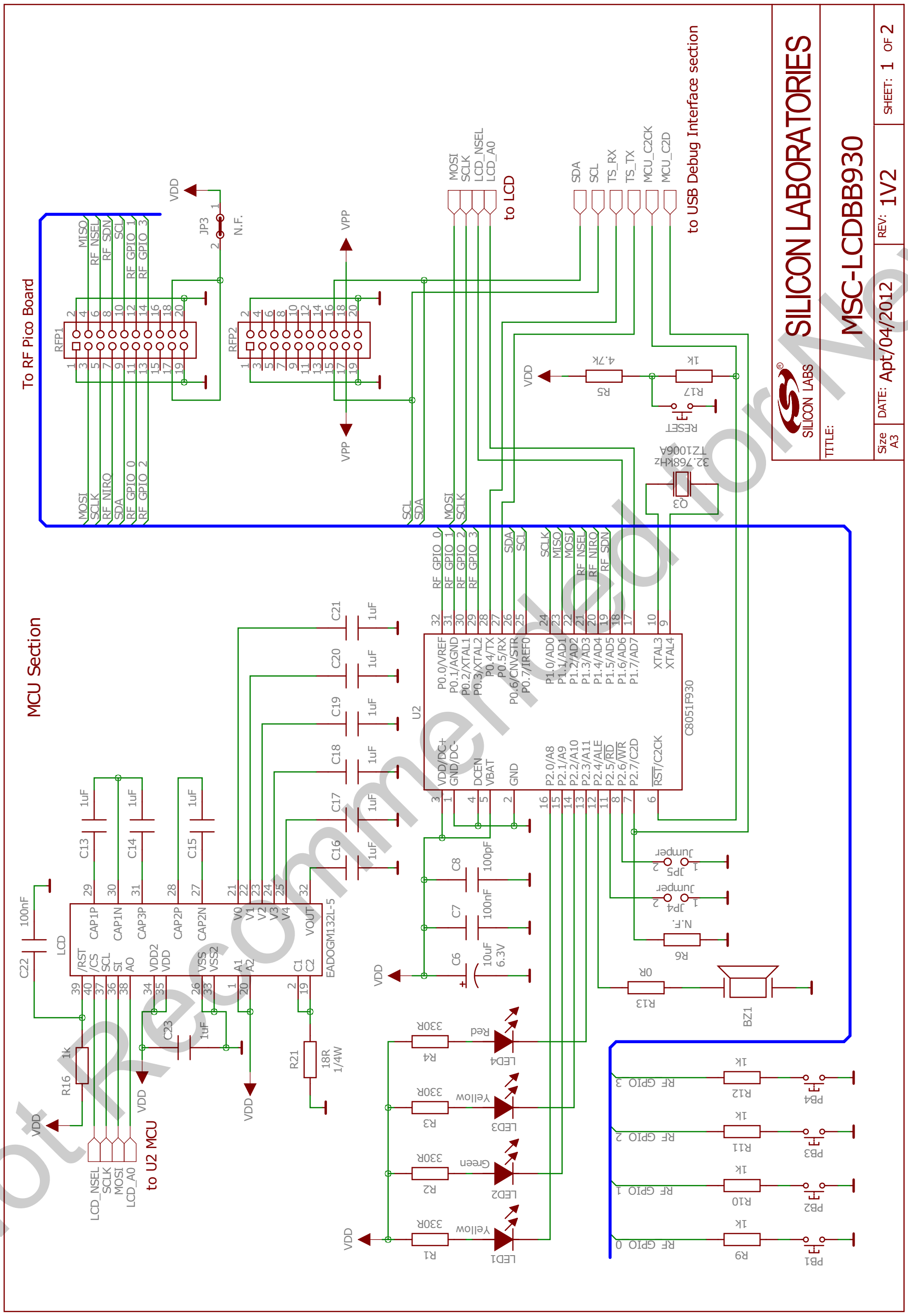


Figure 15. LCD Base Board Schematic 1

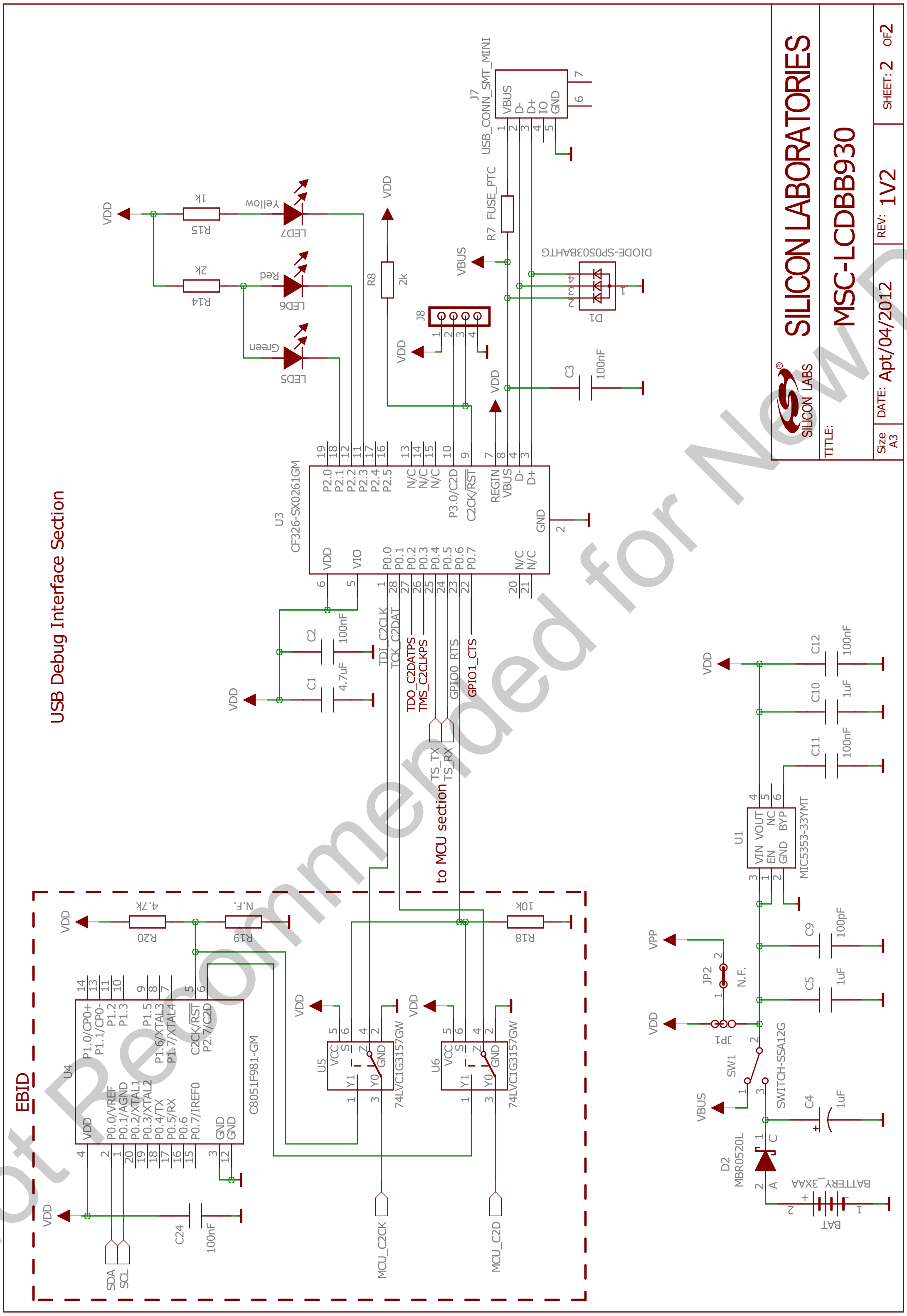


Figure 16. LCD Base Board Schematic 2

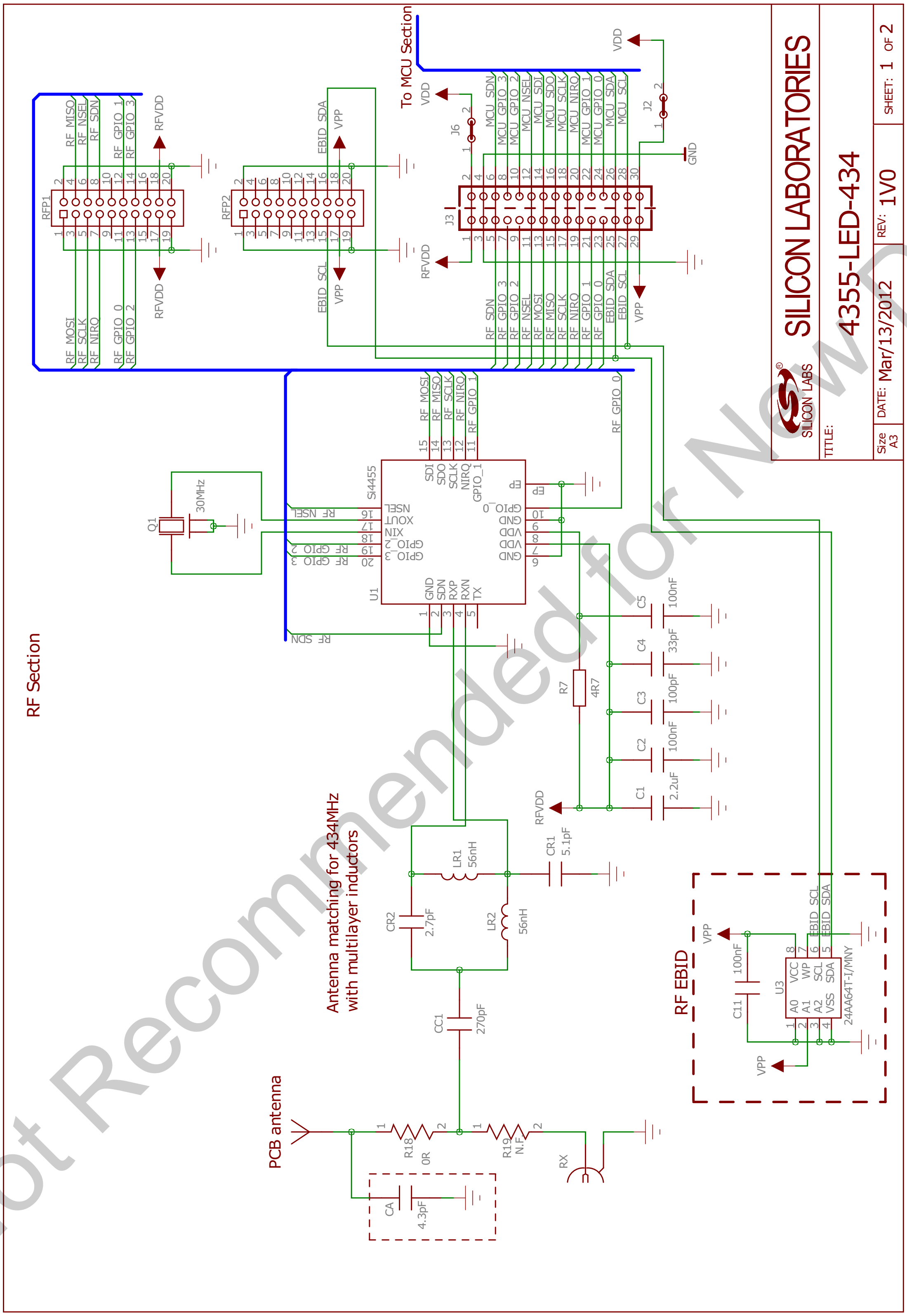


Figure 17. RFPico Board Schematic

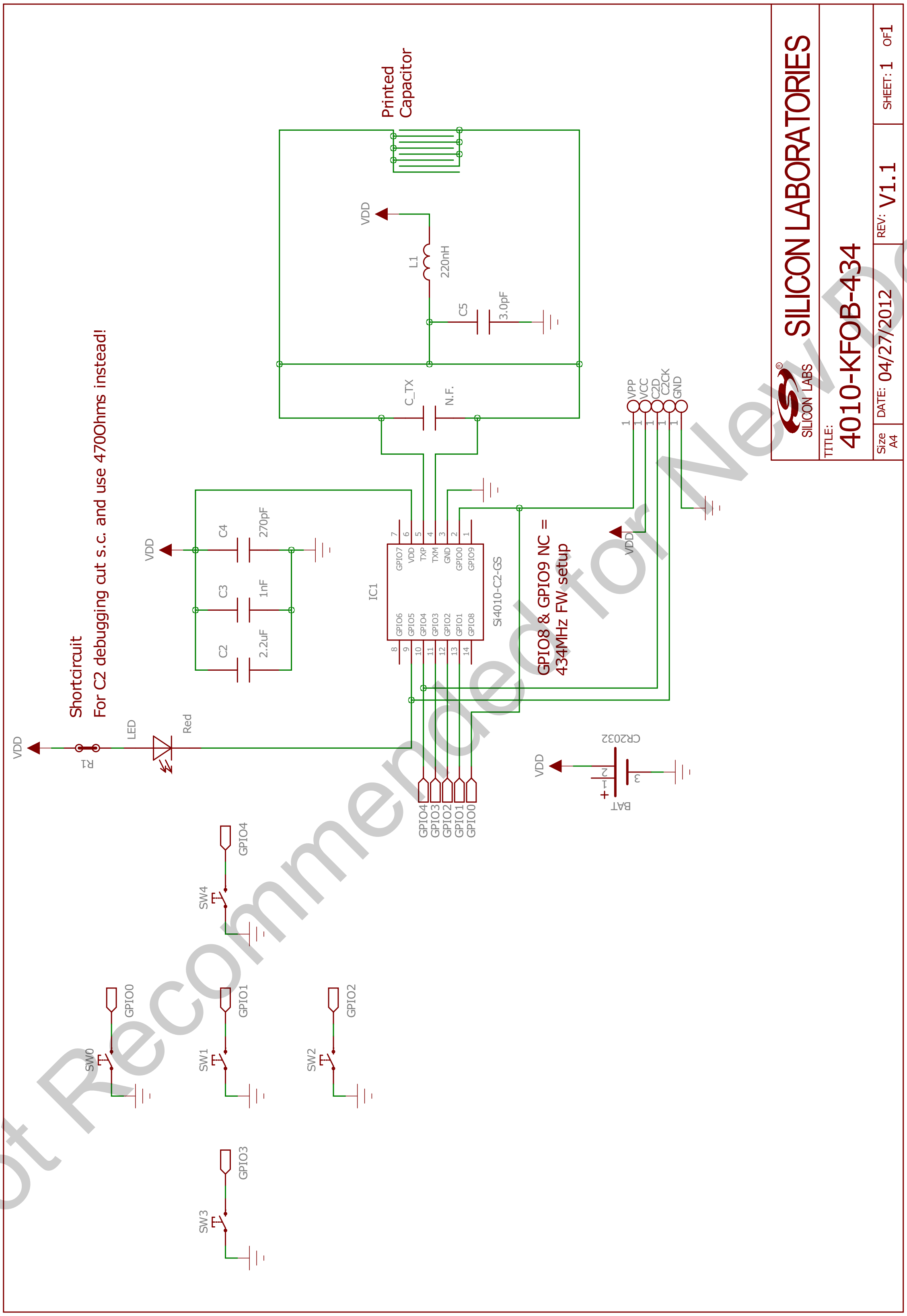


Figure 18. Si4010-KFOB-434 Schematic

Document Change List

Revision 0.1 to Revision 0.2

- Added schematic diagrams.
- Modified the purpose description.

NOTES:

Simplicity Studio

One-click access to MCU tools, documentation, software, source code libraries & more. Available for Windows, Mac and Linux!

www.silabs.com/simplicity

MCU Portfolio
www.silabs.com/mcu

SW/HW
www.silabs.com/simplicity

Quality
www.silabs.com/quality

Support and Community
community.silabs.com

Disclaimer
Silicon Laboratories intends to provide customers with the latest, accurate, and in-depth documentation of all peripherals and modules available for system and software implementers using or intending to use the Silicon Laboratories products. Characterization data, available modules and peripherals, memory sizes and memory addresses refer to each specific device, and "Typical" parameters provided can and do vary in different applications. Application examples described herein are for illustrative purposes only. Silicon Laboratories reserves the right to make changes without further notice and limitation to product information, specifications, and descriptions herein, and does not give warranties as to the accuracy or completeness of the included information. Silicon Laboratories shall have no liability for the consequences of use of the information supplied herein. This document does not imply or express copyright licenses granted hereunder to design or fabricate any integrated circuits. The products must not be used within any Life Support System without the specific written consent of Silicon Laboratories. A "Life Support System" is any product or system intended to support or sustain life and/or health, which, if it fails, can be reasonably expected to result in significant personal injury or death. Silicon Laboratories products are generally not intended for military applications. Silicon Laboratories products shall under no circumstances be used in weapons of mass destruction including (but not limited to) nuclear, biological or chemical weapons, or missiles capable of delivering such weapons.

Trademark Information
Silicon Laboratories Inc., Silicon Laboratories, Silicon Labs, SiLabs and the Silicon Labs logo, CMEMS®, EFM, EFM32, EFR, Energy Micro, Energy Micro logo and combinations thereof, "the world's most energy friendly microcontrollers", Ember®, EZLink®, EZMac®, EZRadio®, EZRadioPRO®, DSPLL®, ISOmodem ®, Precision32®, ProSLIC®, SiPHY®, USBXpress® and others are trademarks or registered trademarks of Silicon Laboratories Inc. ARM, CORTEX, Cortex-M3 and THUMB are trademarks or registered trademarks of ARM Holdings. Keil is a registered trademark of ARM Limited. All other products or brand names mentioned herein are trademarks of their respective holders.

SILICON LABS®

Silicon Laboratories Inc.
400 West Cesar Chavez
Austin, TX 78701
USA

http://www.silabs.com