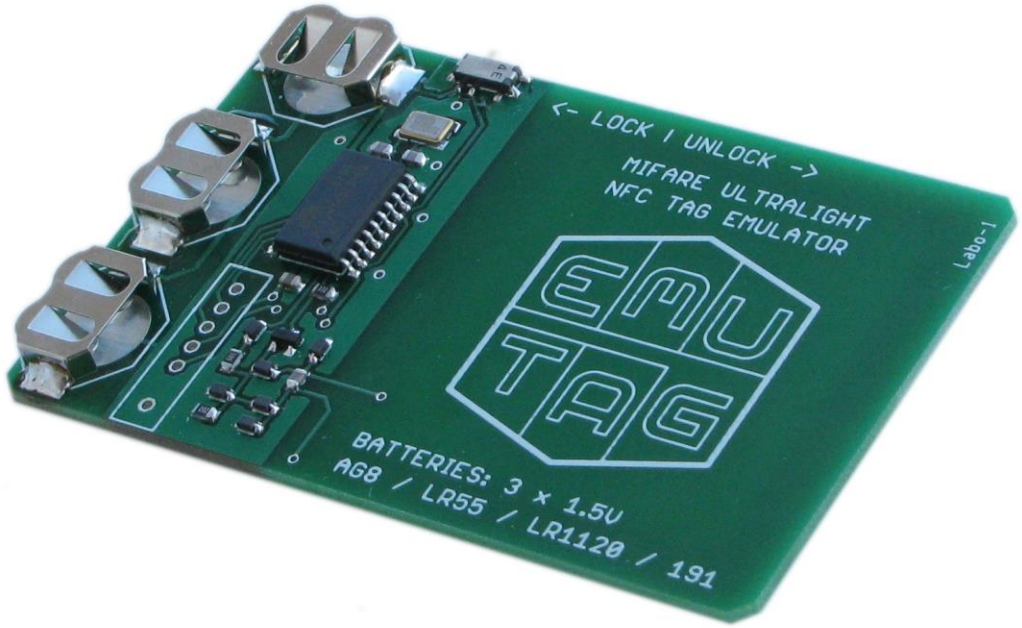
MIFARE ULTRALIGHT NFC TAG EMULATOR

Device Datasheet and Instruction Manual



General Product Description

This Emulator has been designed to be a functional clone of NFC chip MF0ICU1 [1] used in NFC tags (proximity integrated circuit cards). The Emulator also includes a built-in coil antenna, making it a complete standalone solution for emulating MIFARE Ultralight NFC tags, conforming to ISO 14443-A standard (parts 1-3) and operating at 13.56 MHz frequency. In addition to replicating the wireless interface of MF0ICU1 and its memory architecture, the Emulator offers additional features of programming a custom UID, manufacturer byte, internal data byte, as well as resetting OTP bits, lock bits, and block-locking bits to their initial state of logic 0. This makes the Emulator ideal for software development, system testing, and application support, in cases where project development or system administration require many test-case scenarios involving memory areas with security restrictions. With a flip of a switch, the Emulator is turned from a functional clone into a fully writable 64-byte memory array, and vice-versa[1].

[1] — 3 bytes out of 64 always have restrictions on writing, required by ISO 14443-A standard, part 3.

Hardware Features:

- **Antenna on flat bottom side, allowing zero minimum separation from reader**
- **Shielded electronic section outside of antenna area, reducing interference**
- **Meets and exceeds ISO 14443-A requirements on wireless performance**
- **Emulates electromagnetic load on proximity coupling device antenna field**
- **Implements automatic power saving when antenna field is not present**

Software Features:

- **Supports anti-collision**
- **Supports parity generation and checking**
- **Supports CRC generation and checking**
- **Supports all MF0ICU1 commands and replicates its state diagram**
- **Replicates all timings of MF0ICU1 with precision of 1 carrier cycle**

With switch set to Locked position:

- **Replicates security behaviour of OTP, lock, and block-locking bits**
- **Replicates ACK/NAK answers to WRITE and COMPATIBILITY_WRITE commands**

With switch set to Unlocked position:

- **Allows writing UID, manufacturer, and internal bytes**
- **Allows clearing and setting OTP, lock, and block-locking bits independently**

Functional Description

The Emulator has a switch that can be toggled between one of the two positions: Locked and Unlocked. In the Locked mode, the Emulator operates according to the MF0ICU1 chip datasheet [1], with a few possible exceptions that can be programmed in the Unlocked mode:

- Manufacturer byte 0 of page 0 (UID0) can be different from 0x04. It can be freely changed in Unlocked mode, and its value is stored with no change when the switch is moved to the Locked mode.

> **WARNING!** Changing the manufacturer byte might render the Emulator unreadable with some hardware or software applications designed to communicate with MIFARE Ultralight tags. If such a situation occurs, the entire memory content can be restored back to initial state (see Table 1) by removing at least one battery and inserting it back after more than 2 seconds.

- Internal data byte 1 of page 2 can be different from 0x48. Similarly to the manufacturer byte, it can be freely changed in Unlocked mode, and its value is stored with no change when the switch is moved to the Locked mode.

> **WARNING!** Normally, the internal data byte is not designed to carry information, since it is locked to a constant in real MIFARE Ultralight tags. In most applications, changing the internal data byte does not affect normal operation of the tag. However, if the Emulator becomes unreadable after changing the internal data byte, the entire memory content can be restored back to initial state (see Table 1) by removing at least one battery and inserting it back after more than 2 seconds.

In the Unlocked mode, all 16 pages are fully writable, with the following exceptions:

- Byte 3 of page 0 (BCC0) always reads the value equal to UID0 ⊕ UID1 ⊕ UID2 ⊕ 0x88 (see Table 2), according to ISO 14443-A part 3. Writing an arbitrary value to byte 3 of page 0 has no effect, and write operations to page 0 always return a positive acknowledge ACK. This allows the user (software) to avoid calculating the value of BCC0, and is convenient for manual UID entry.
- Byte 0 of page 1 (UID3) can not be written with value 0x88. If a WRITE (0xA2) command is issued, where byte 0 is 0x88, a NAK is immediately returned and the entire page remains unchanged in the memory array. If a COMPATIBILITY_WRITE command is issued to page 1, the response is always ACK for the first part of the command. For the second part, if byte 0 is 0x88, a NAK is immediately returned and the entire page remains unchanged in the memory array.
- Byte 0 of page 2 (BCC1) always reads the value equal to UID3 ⊕ UID4 ⊕ UID5 ⊕ UID6 (see Table 2), according to ISO 14443-A part 3. Writing an arbitrary value to byte 0 of page 2 has no effect, and write operations to page 2 always return a positive acknowledge ACK. This allows the user (software) to avoid calculating the value of BCC1, and is convenient for manual UID entry.

These restrictions are always present, and are necessary to keep the Emulator readable. Lack of these restrictions could render the Emulator unreadable both in practice and according to ISO 14443-A part 3.

Table 1: Initial Memory State

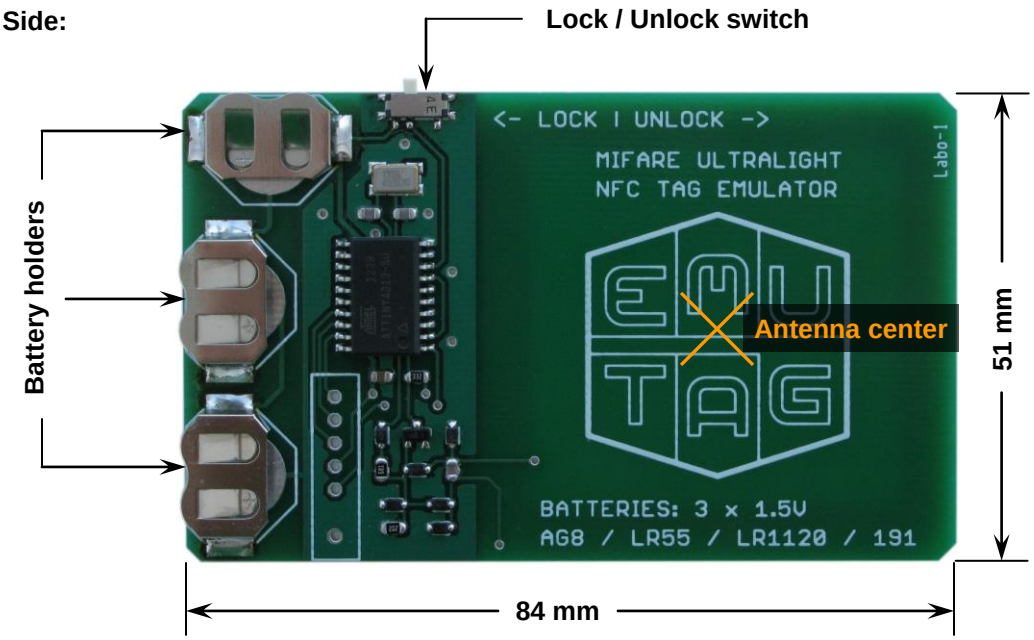
	Byte 0	Byte 1	Byte 2	Byte 3
Page 0	04	00	00	8C
Page 1	00	00	00	00
Page 2	00	48	00	00
Page 3	00	00	00	00
Page 4	FF	FF	FF	FF
Page 5	00	00	00	00
Page 6	00	00	00	00
Page 7	00	00	00	00
Page 8	00	00	00	00
Page 9	00	00	00	00
Page 10	00	00	00	00
Page 11	00	00	00	00
Page 12	00	00	00	00
Page 13	00	00	00	00
Page 14	00	00	00	00
Page 15	00	00	00	00

Table 2: Reserved Byte Definitions

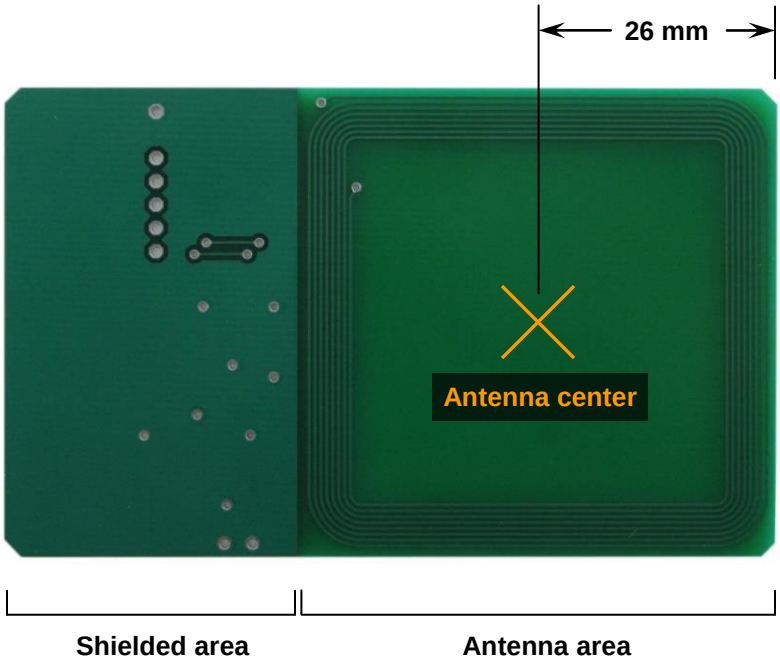
	Byte 0	Byte 1	Byte 2	Byte 3
Page 0	UID0	UID1	UID2	BCC0
Page 1	UID3	UID4	UID5	UID6
Page 2	BCC1	Internal		

Physical Dimensions and Component Locations

Top Side:



Bottom Side:



Device thickness is 5 mm.

Power Supply Requirements

The Emulator is powered from 3 batteries 1.5V each. Batteries are included when the device is shipped. The isolator paper with the "PULL" label needs to be removed before use.

Compatible batteries are known under the following names:
AG8, SG8, LR55, SR55, LR1120, SR1120, 191, 381, 391.

The correct battery orientation is with positive side upwards. The smaller (negative) battery terminal should touch the printed circuit board.

The Emulator does not have a power switch, and it does not need any, since its automatic power saving feature reduces power consumption to almost zero when the electromagnetic field of a reader is not acting on the antenna. Batteries are needed to keep the memory state of the emulated NFC tag. If any of the three batteries is removed, the memory content of the emulated tag is reverted back to the initial state (see Table 1) when the power is provided the next time, independent of the switch position. The electrical power parameters are provided in Table 3.

Electrical Characteristics

Table 3: Electrical Specifications

Parameter	Min.	Typ.	Max.	Unit
Operating voltage	3.3	-	5.5	V
Battery current consumption (reader field present)	-	5.6	7.1	mA
Battery current consumption (no reader field)	-	0.2	2.1	µA
Carrier signal frequency	-	13.56	-	MHz
Emulator crystal frequency deviation	-	-	20	ppm
Reader frequency deviation	-	-	50	ppm
Antenna input capacitance	-	18	-	pF
Operating temperature	0	-	+60	°C
Storage temperature (no batteries)	–40	-	+85	°C

NFC Reader Compatibility

Any reader compatible with standard MIFARE Ultralight tags is also compatible with the Emulator.

List of Recommended Android Software

MIFARE++, UltraManager, NFC Tag maker, RFID Tool, NFC TagInfo, and others.

Trademarks

All referenced brands, product names, service names and trademarks are the property of their respective owners.

MIFARE — is a trademark of NXP Semiconductors N.V.

MIFARE Ultralight — is a trademark of NXP Semiconductors N.V.

Warranty

Every Emulator is individually tested for electrical connections and for operation before shipping. The Emulator comes with NO WARRANTY, but technical support may be provided in future. NFC knowledge is recommended when using the Emulator.

Disclamer

The manufacturer can not be held responsible for any consequences that may arise while or after using the Emulator. The user or developer holds the ultimate responsibility in application design or use of the Emulator. All use is at customer's own risk.

References

[1] MF0ICU1 — http://www.nxp.com/documents/data_sheet/MF0ICU1.pdf

[2] ISO 14443-2 — http://jpkc.szpt.edu.cn/2007/sznk/UploadFile/biaozhun/iso14443/14443-2.pdf

[3] ISO 14443-3 — http://jpkc.szpt.edu.cn/2007/sznk/UploadFile/biaozhun/iso14443/14443-3.pdf