ROWLAND’s Research: Version 2.0

# 

# Research: Preliminary

# 

## Flipper youtube: <https://www.youtube.com/flipperzero>

# 

## [Demonstration] Flipper Zero: Hottest Hacking Device for 2023? [Flipper Zero: Hottest Hacking Device for 2023? - YouTube](https://www.youtube.com/watch?v=VF3xlAm_tdo)

### Flipper zero can be used to copy some info from RFID-supported devices, like credit cards and ID cards, to enable the use of the info (if it is not encrypted). In the video, he locks an electronic hotel lock using a credit card. He then uses Flipper Zero to copy the card card info. Then, he uses the Flipper Zero as an emulator to unlock the hotel lock.

#### Solution: Placing a RFID blocking card to overlap a credit card prevents Flipper Zero from reading the card’s electronic tag.

### Controlling Infrared devices: Flipper Zero can be used to copy an infrared configuration from an infrared remote control, enabling the Flipper Zero to be used to replicate the production and performance of the function of that Infrared wavelength, including tv, air-conditioner and coloured lights, remote controls.

### Emulate PC Mouse: Can be used to emulate a bluetooth mouse on a computer, as well as any other bluetooth device. In the demonstration, using it’s directional control and select keys, Flipper Zero is used to control a computer’s pointer via bluetooth.

### Bad USB: Flipper zero can be used to run Rubber Ducky scripts. The demonstration shows Flipper zero writing some characters to a file. Many more functions can be performed after downloading Rubber Ducky scripts from [nocomp/Flipper\_Zero\_Badusb\_hack5\_payloads: hack5 badusb payloads moded for be played with flipper zero (github.com)](https://github.com/nocomp/Flipper_Zero_Badusb_hack5_payloads) to do things, such as opening up a reverse shell.

#### A shell is a user interface for access to operating system services.

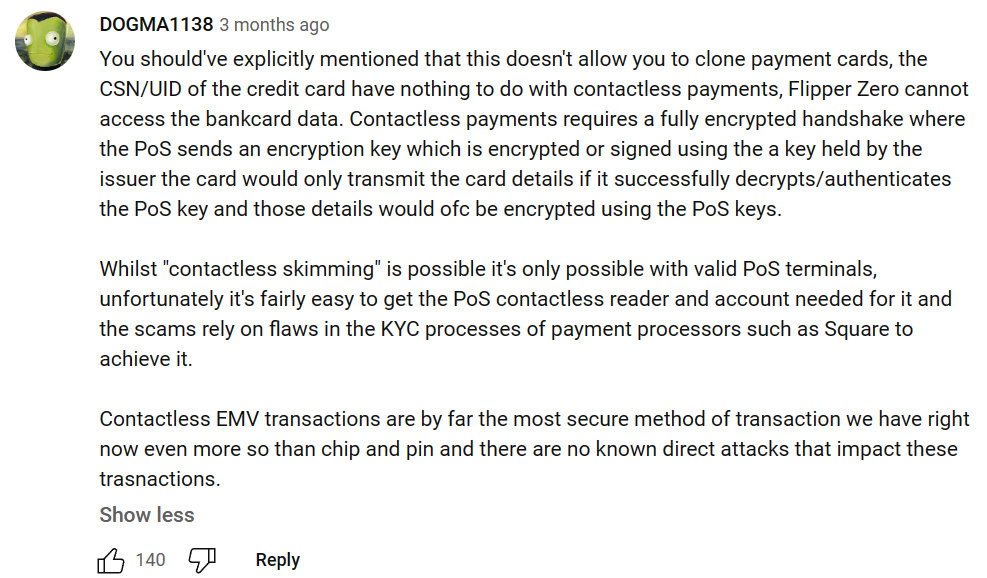
#### A **reverse shell** is a remote shell, where the connection is made from the system that offers the services to the client that wants to use these services. Attackers can also use web shells instead of reverse shells.

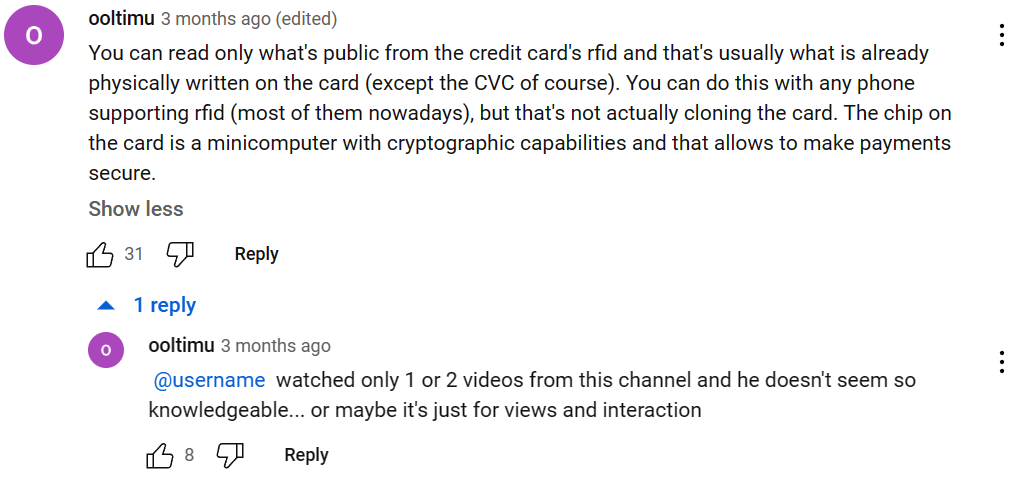
### Remotely control Flipper zero: Can be synced to another device, such as a mobile phone or a computer, from which the Flipper Zero can be remotely controlled using software.

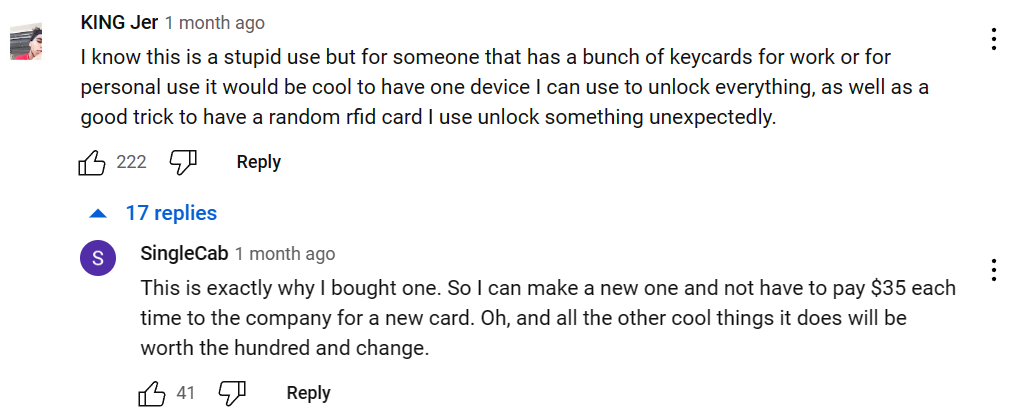
### NFC on Flipper zero can be use to read a Yubikey.

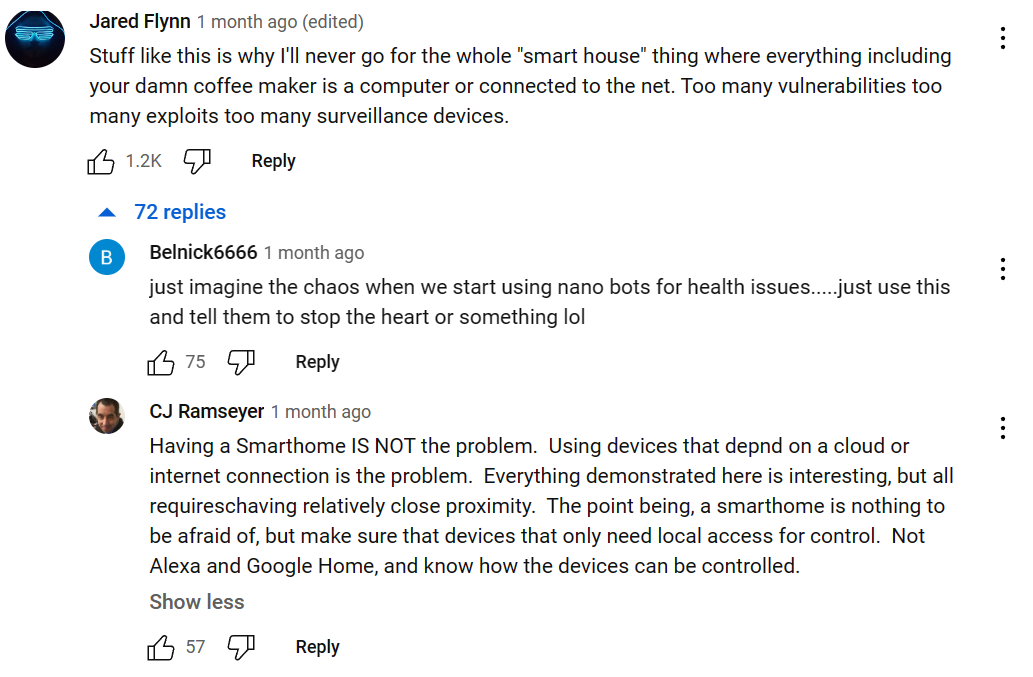
#### The YubiKey is a hardware authentication device manufactured by Yubico to protect access to computers, networks, and online services that supports one-time passwords, public-key cryptography, and authentication, and the Universal 2nd Factor and FIDO2 protocols developed by the FIDO Alliance. It allows users to securely log into their accounts by emitting one-time passwords or using a FIDO-based public/private key pair generated by the device. YubiKey also allows for storing static passwords for use at sites that do not support one-time passwords.

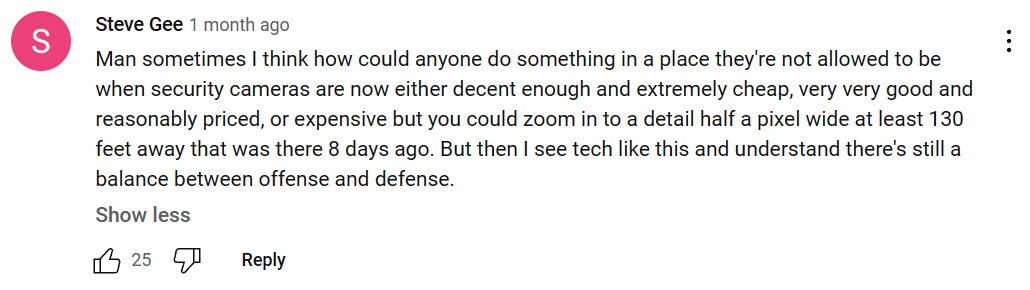
### Valuable Youtube comments

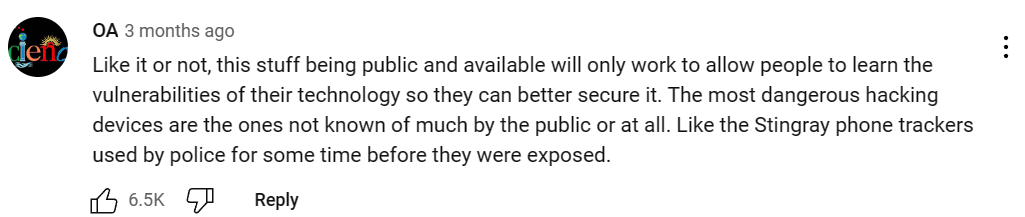


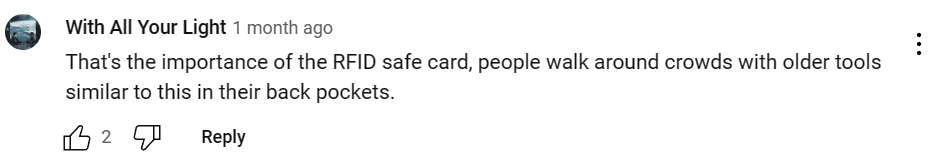


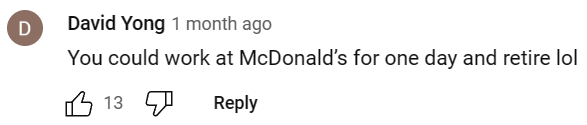


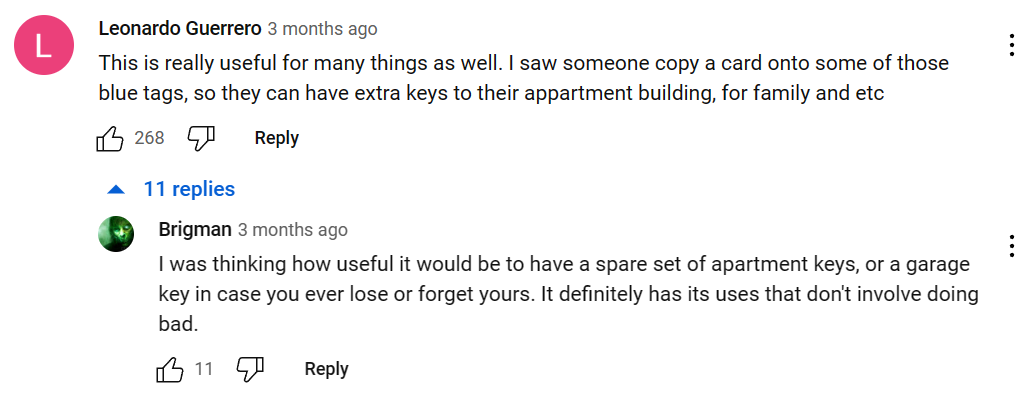






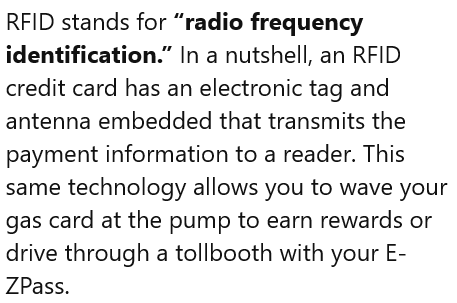






## RFID [definitions and theory]

**Radio-frequency identification** uses electromagnetic fields to automatically identify and track tags attached to objects. An RFID system consists of a tiny radio transponder, a radio receiver and transmitter. When triggered by an electromagnetic interrogation pulse from a nearby RFID reader device, the tag transmits digital data, usually an identifying inventory number, back to the reader. This number can be used to track inventory goods.

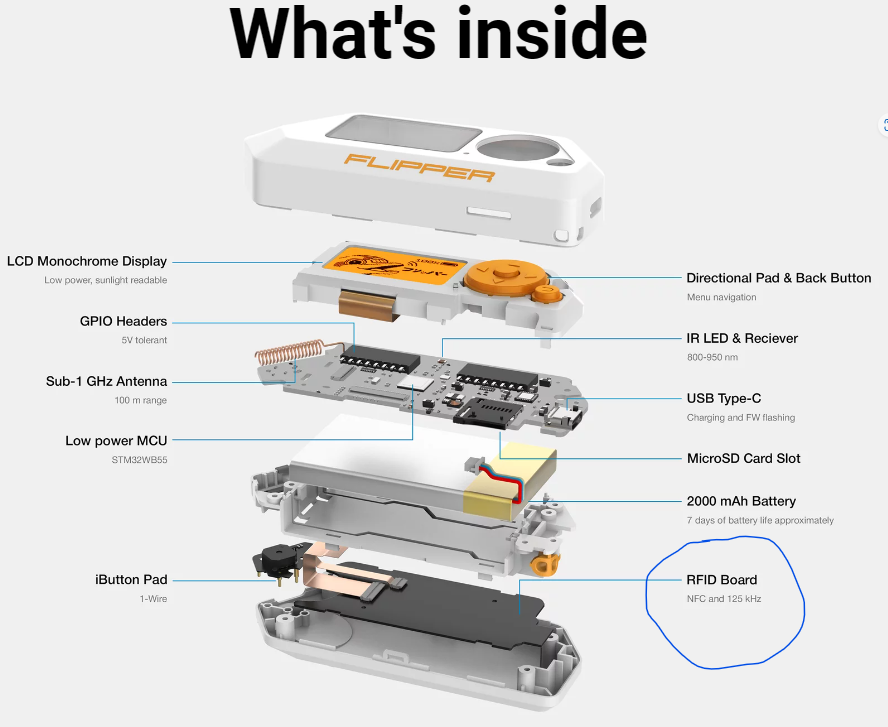


## NFC [definitions and theory]

**Near field communication**: a technology allowing the short-range wireless intercommunication of mobile phones and other electronic devices for purposes such as making payments

# Research: Flipper Zero and RFID Intro

[Flipper Zero — Portable Multi-tool Device for Geeks](https://flipperzero.one/)





## 125 kHz RFID - Low-frequency proximity cards

[Flipper Zero — Portable Multi-tool Device for Geeks](https://flipperzero.one/)

This type of card is widely used in old access control systems around the world. It's pretty dumb, stores only an N-byte ID and has no authentication mechanism, allowing it to be read, cloned and emulated by anyone. A 125 kHz antenna is located on the bottom of Flipper — it can read EM-4100 and HID Prox cards, save them to memory to emulate later.

You can also emulate cards by entering their IDs manually.

Moreover, Flipper owners can exchange card IDs remotely.

## NFC - High-frequency proximity cards

[Flipper Zero — Portable Multi-tool Device for Geeks](https://flipperzero.one/)

Flipper Zero has a built-in NFC module (13.56 MHz). Along with the 125kHz module, it turns Flipper into an ultimate RFID device operating in both Low Frequency (LF) and High Frequency (HF) ranges. The NFC module supports all the major standards.

It works pretty much the same as the 125 kHz module, allowing you to interact with NFC-enabled devices — read, write and emulate HF tags.

# Research: 125 kHz RFID - Low-frequency proximity cards

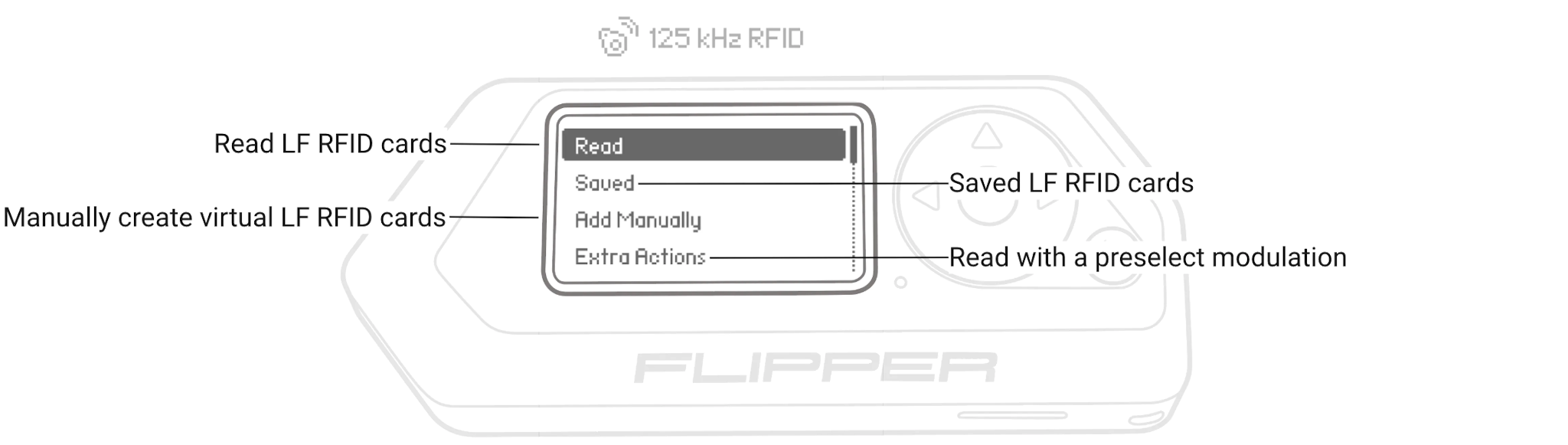
[125 kHz RFID - Flipper Zero — Documentation](https://docs.flipperzero.one/rfid)



Flipper Zero supports low-frequency (LF) radio frequency identification (RFID) technology that is implemented in access control systems, animal chips, and supply chain tracking systems. Unlike NFC cards, LF RFID cards usually do not provide high levels of security. This technology comes in many form-factors, such as plastic cards, key fobs, tags, wristbands, and animal microchips. Flipper Zero has a low-frequency RFID module capable of reading, saving, emulating, and writing LF RFID cards.

## 125 kHz RFID menu - See [125 kHz RFID - Flipper Zero — Documentation](https://docs.flipperzero.one/rfid)

You can access the 125 kHz RFID application from the Main Menu. In the application, you can read, save, emulate, write, and generate new LF RFID cards.



### ﻿Read — reads and saves LF RFID cards.

* + [Reading 125 kHz RFID cards - Flipper Zero — Documentation](https://docs.flipperzero.one/rfid/read)
  + [Animal microchips - Flipper Zero — Documentation](https://docs.flipperzero.one/rfid/animal-microchips)

### Saved — lists saved cards that can be emulated and written on an empty card.

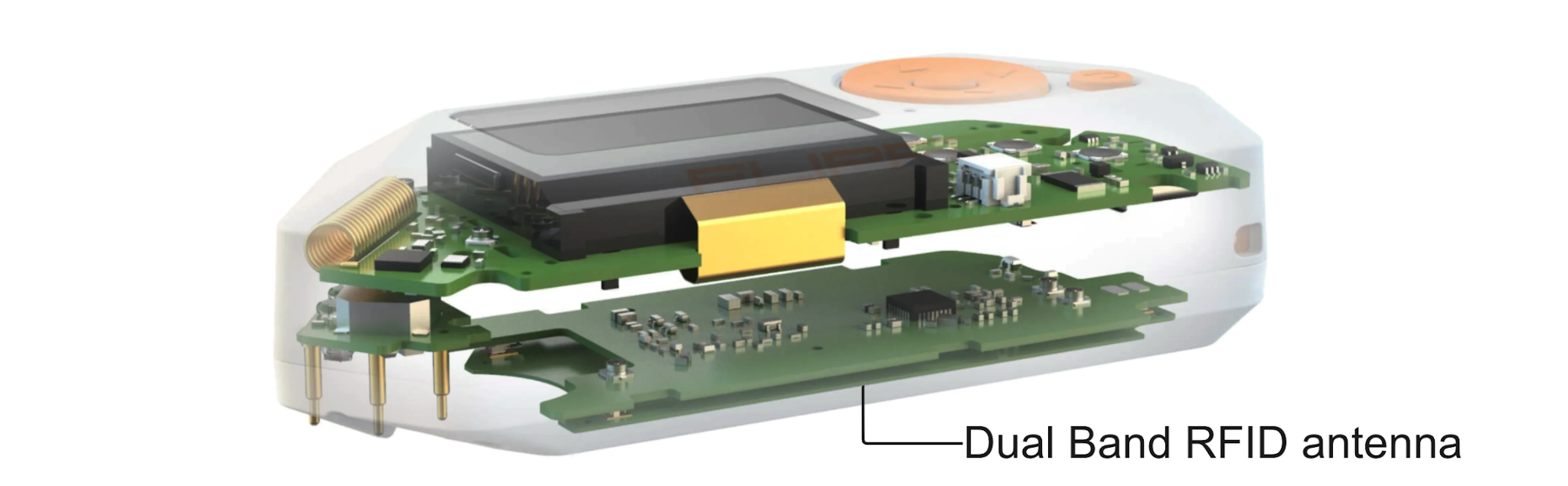
### ﻿Add Manually — generates new virtual LF RFID cards by entering the cards' ID.

* + [Adding 125 kHz cards manually - Flipper Zero — Documentation](https://docs.flipperzero.one/rfid/add-manually)

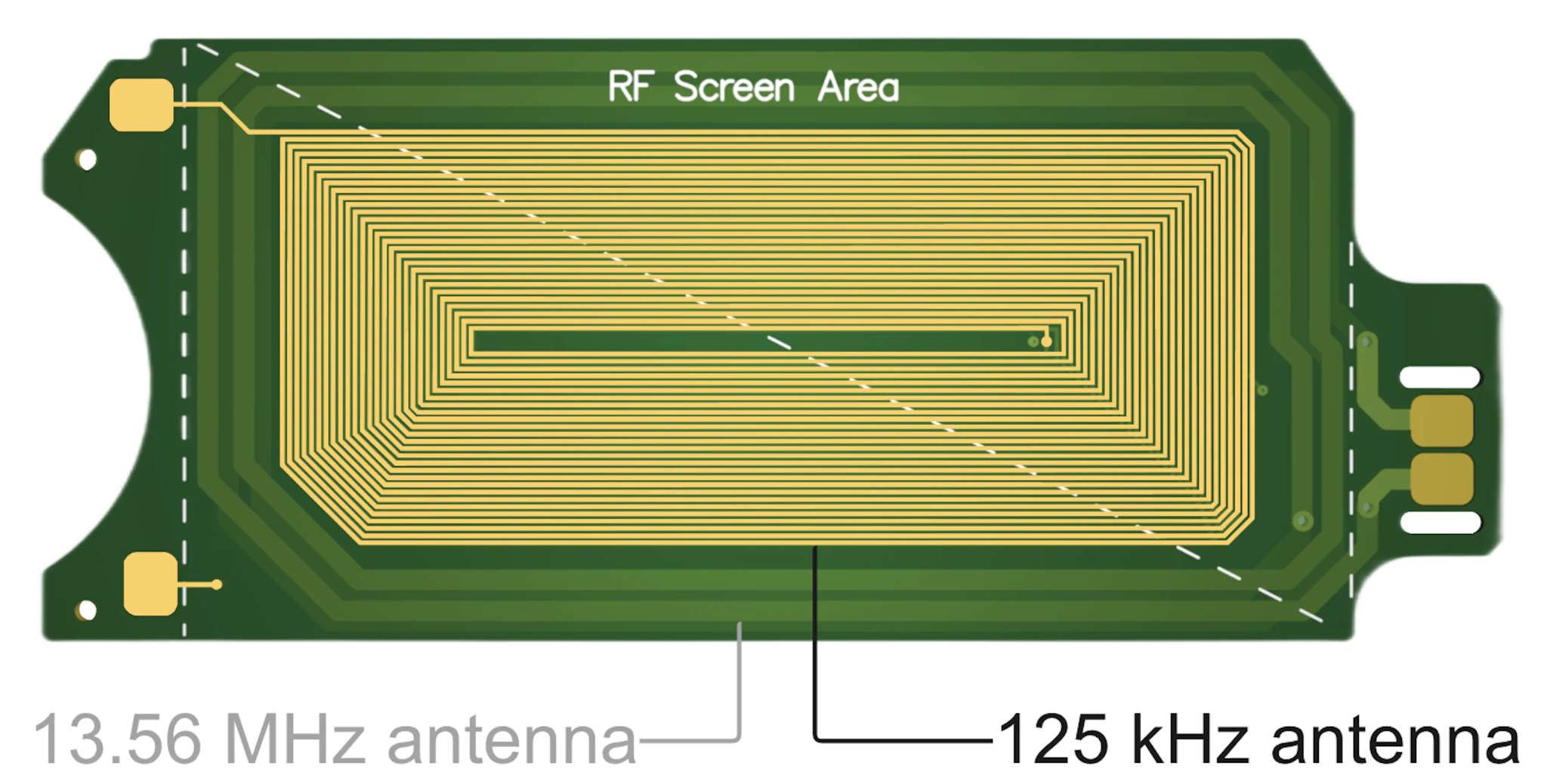
### Extra Actions — allows to reading LF RFID cards with the preselected ASK or PSK coding.

## 125 kHz RFID hardware - See [125 kHz RFID - Flipper Zero — Documentation](https://docs.flipperzero.one/rfid)

Flipper Zero has a built-in RFID support with a low-frequency antenna located at the back of Flipper Zero. The STM32WB55 microcontroller unit is used for the 125 kHz RFID functionality.



The low-frequency 125 kHz antenna is placed on the Dual Band RFID antenna next to the high-frequency 13.56 MHz antenna.



## Flipper Zero schematics - See [Flipper Zero schematics - Flipper Zero — Documentation](https://docs.flipperzero.one/development/hardware/schematic)

﻿

## 125 kHz RFID application source code - See [flipperzero-firmware/applications/main/lfrfid at dev · flipperdevices/flipperzero-firmware (github.com)](https://github.com/flipperdevices/flipperzero-firmware/tree/dev/applications/main/lfrfid)

# Extra

Flipper Devices - Flipper Zero project sources - [Flipper Devices (github.com)](https://github.com/flipperdevices)

Design guide - [Design Guide (flipperzero.one)](https://flipperzero.one/design-guide)