Version 1.0

# Research: Preliminary and some extract from file “Credit Card RF”

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

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

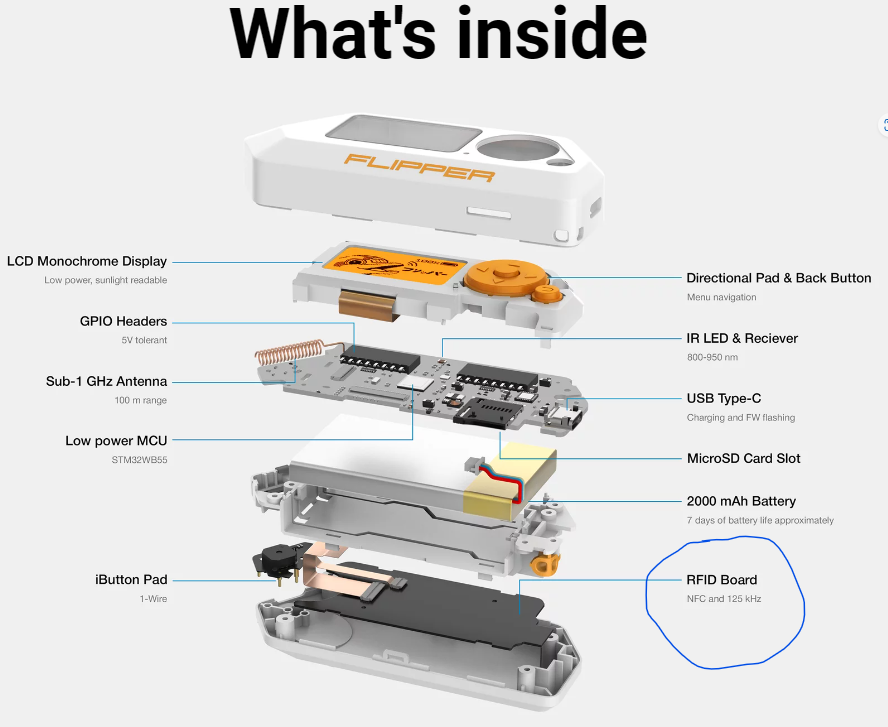
#### The YubiKey is a hardware authentication device manufactured by Yubico to protect access to computers, networks, and online services that supports one-time passwords, public-key cryptography, and authentication, and the Universal 2nd Factor and FIDO2 protocols developed by the FIDO Alliance. It 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.

## 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 NFC Intro

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





## NFC - High-frequency proximity cards

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

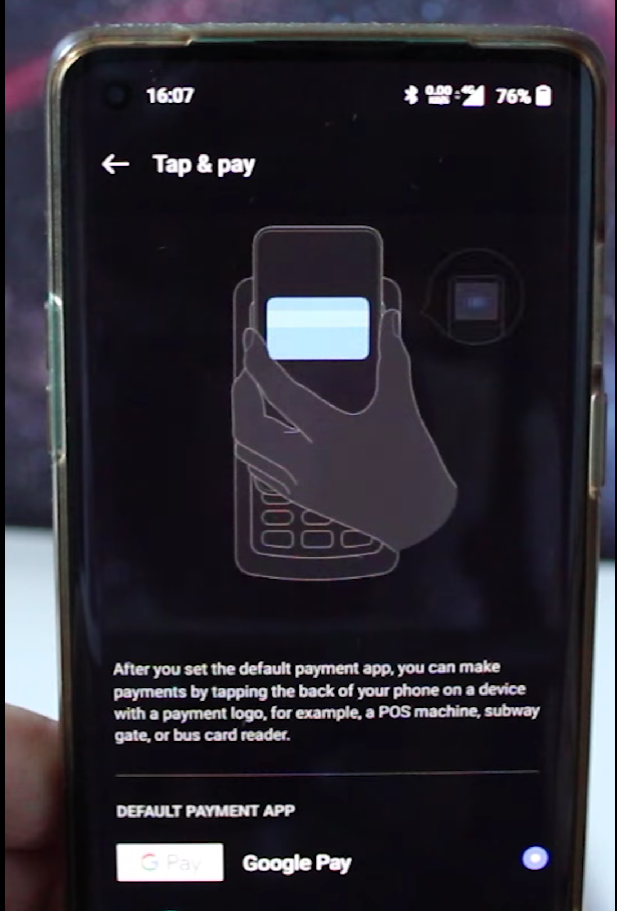
Flipper Zero has a built-in NFC module (13.56 MHz). Along with the 125kHz module, it turns Flipper into an ultimate RFID device operating in both Low Frequency (LF) and High Frequency (HF) ranges. The NFC module supports all the major standards.

[What is NFC and how does it work? Here's everything you need to know (androidauthority.com)](https://www.androidauthority.com/what-is-nfc-270730/)

1. Has a maximum data transfer rate of 424 kilo bits per second.
2. Usually it is most effective in operation in ranges not greater than a few centimeters
3. Found in smartphones, tablets and gaming consoles such as nintendo switch.



* 1. In mobile devices, it is used by some payment systems such as google pay and apple pay



c. Ticketing systems for rapidly pairing headphones or bluetooth speakers with smartphones

d. NFCs always involve at least 2 functional devices; Initiator and Target.

The initiator generates an electromagnetic field using an electromagnetic coil and inductive coupling to exchange data

e. Android has supported NFC since 2010 especially in mid to high end phones and iPhone 6 and newer iPhones also support NFC.

f. NFC isn’t some radically new technology. It’s simply an evolution of [RFID](https://www.androidauthority.com/what-is-rfid-975910/) (radio frequency identification) technology that has already been around for decades. If you’ve ever used a key card to access an office building or hotel room, you’re already familiar with how it works.

Both RFID and NFC operate on the principle of inductive coupling, at least for short-range implementations. This essentially involves the reader device generating a magnetic field by passing an electric current through a coil. When a tag (with its own coil) is brought nearby, the field induces an electric current within the tag — sans any wires or even physical contact. Then, once the initial handshake is complete, any stored data on the tag is wirelessly transmitted to the reader.

***NFC is based on RFID technology, but has a much lower transmission range.***

The key distinction between RFID and NFC lies in their transmission ranges — the former is often used over longer distances. For example, some regions automatically collect road tolls through RFID. Tags are usually affixed to vehicle windshields and you simply have to drive through the toll booth. Communication can take place over even longer distances (think a hundred feet or more) if the RFID tag is equipped with a power source.

NFC, however, only has a maximum range of a few centimeters, at most. And in most smartphone-related applications, you’ll find that the software will only initiate communication if there’s physical contact. This is to prevent accidental triggers — especially important now that the technology is used for transferring sensitive data.

Another noteworthy point is that NFC devices can act as either a reader or tag. This bidirectional capability allows you to use one piece of hardware — such as your smartphone — for all kinds of different applications.

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.

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.

### Common Applications of NFC:

**Public transport access**: Public transport in many cities, including Edmonton, Hong Kong, Singapore, and London, use NFC-based cards as a form of access control mechanism for public transit. Some systems are even compatible with payment apps like Google Pay so you don’t have to carry the card around. One very local use is ARC cards used for public transportation in Edmonton and issued to MacEwan University students.



**Data transfer**: With the release of Android Ice Cream Sandwich in 2011, Google introduced Android Beam. The feature allowed you to transfer whatever content or data you had on-screen to other NFC-enabled devices. All you had to do was touch the back of both devices and accept the transfer prompt. Android Beam was only recently shelved in favor of Nearby Share, which uses Bluetooth and Wi-Fi Direct technologies instead.

**Mobile payments**: [**Samsung Pay**](https://www.androidauthority.com/samsung-pay-everything-you-need-to-know-678123/), Google Pay, and Apple Pay all use your smartphone’s NFC chip for contactless payments. Most debit and credit cards these days already have an NFC tag built-in. The aforementioned apps simply emulate these tags, with permission from the issuing bank or financial institution. Once configured, all you have to do is bring your smartphone or wearable device close to the card reader.

**Quick pairing**: NFC’s convenience extends to devices that don’t have a screen. Many wireless speakers and headphones use it to exchange pairing information with your smartphone. Some cameras also use it to quickly initiate a Wi-Fi Direct connection for easy photo and video transfer.

**Gaming**: Nintendo uses the technology to connect physical toys with video games. An Amiibo is like any other action figure or trading card, except that it also contains an embedded NFC chip. If you bring one of them near a Nintendo Switch or 3DS, it automatically grants you additional characters, levels, or bonus items for a particular game.

**Home automation**: A few smart home platforms, including Home Assistant and [**Apple’s HomeKit**](https://www.androidauthority.com/apple-homekit-3085803/), support NFC as well. Using apps on both Android and iOS, you can configure off-the-shelf [**NFC tags**](https://www.androidauthority.com/nfc-tags-explained-271872/) to control devices or automation.

## Differences between NFC and RFID with applications of NFC

[NFC vs. RFID: What’s the Difference? - YouTube](https://www.youtube.com/watch?v=m0wXeSxQj9I)

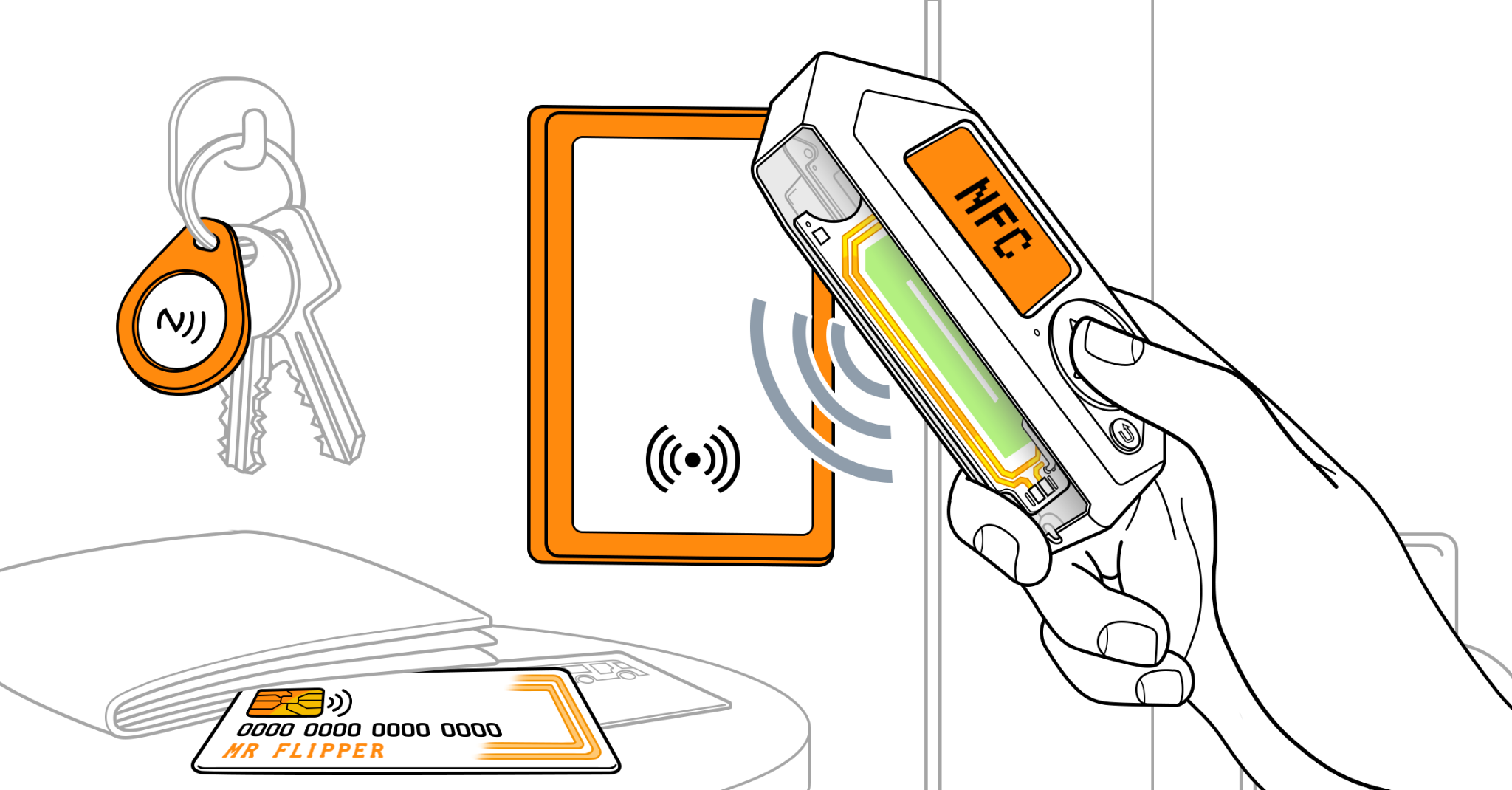
NFC is a subset of RFID although RFID is usually used to refer to the lower frequencies

1. Limited to close range proximity and works well for secure communications such as contactless payments (RFID can be used over long distances making it good for location tracking)
2. Capable of 2-way communication, such as peer to peer mode between devices (RFID is communicates in one direction from the tag to the reader)
3. Has more storage capacity than RFID (RFID usually carries only simple ID info)
4. Usually used for communication involving close contact and handling of the device such as scanning a QR code for Information (RFID is usually used for Identification, including because of it’s higher proximity applications)

See - [How can zero-touch enrollment help Android admins? | TechTarget](https://www.techtarget.com/searchmobilecomputing/answer/How-can-zero-touch-enrollment-help-Android-admins)

# Research: Flipper Zero NFC - High-frequency proximity cards

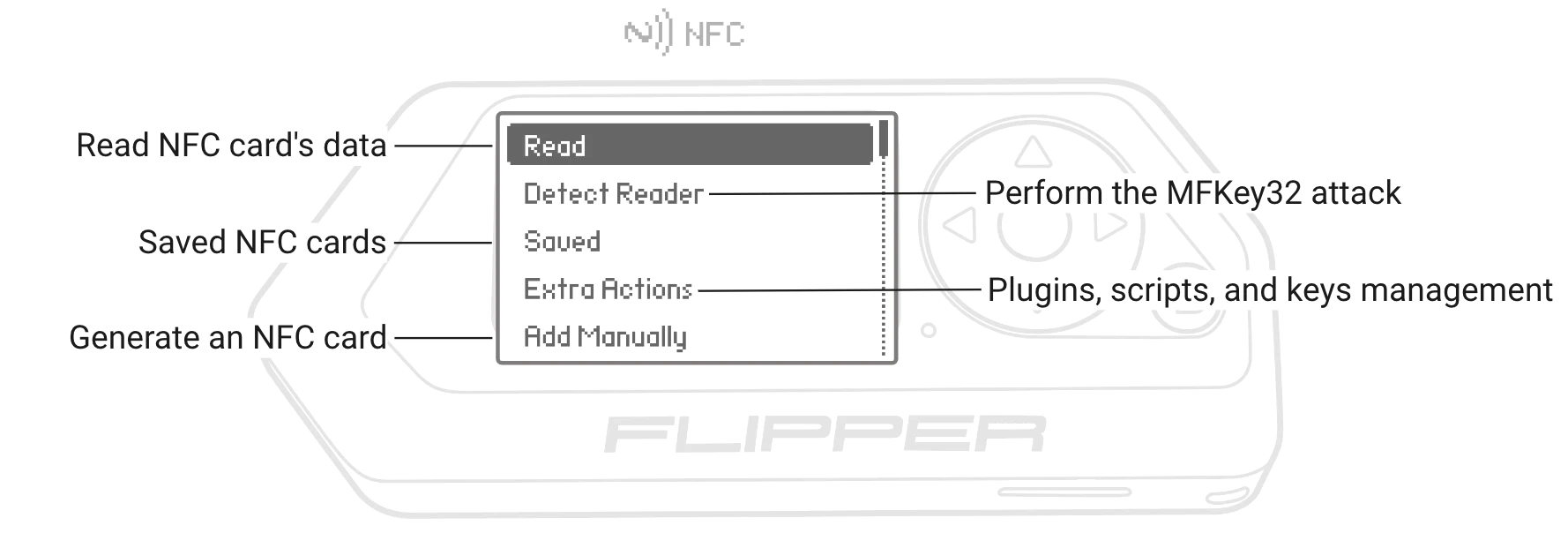
## [NFC - Flipper Zero — Documentation](https://docs.flipperzero.one/nfc)



Flipper Zero supports NFC technology, which is implemented in public transport smart cards, access cards or tags, digital business cards, and bank cards. These cards have complex protocols and support encryption, authentication, and full-fledged two-way data transfer. Flipper Zero has a built-in 13.56 MHz NFC module capable of reading, saving, and emulating NFC cards.

## NFC menu - See [NFC - Flipper Zero — Documentation](https://docs.flipperzero.one/nfc)

You can access the NFC application from the Main Menu. In the application, you can interact with NFC cards, analyze readers, and generate NFC cards.



[**Read**](https://docs.flipperzero.one/nfc/read) — reads and saves NFC card's data such as UID, SAK, ATQA, and stored data.

**Detect Reader** — emulates an MFC 1K card to collect data ([nonces](https://en.wikipedia.org/wiki/Cryptographic_nonce)) used to calculate keys attempted by a reader.

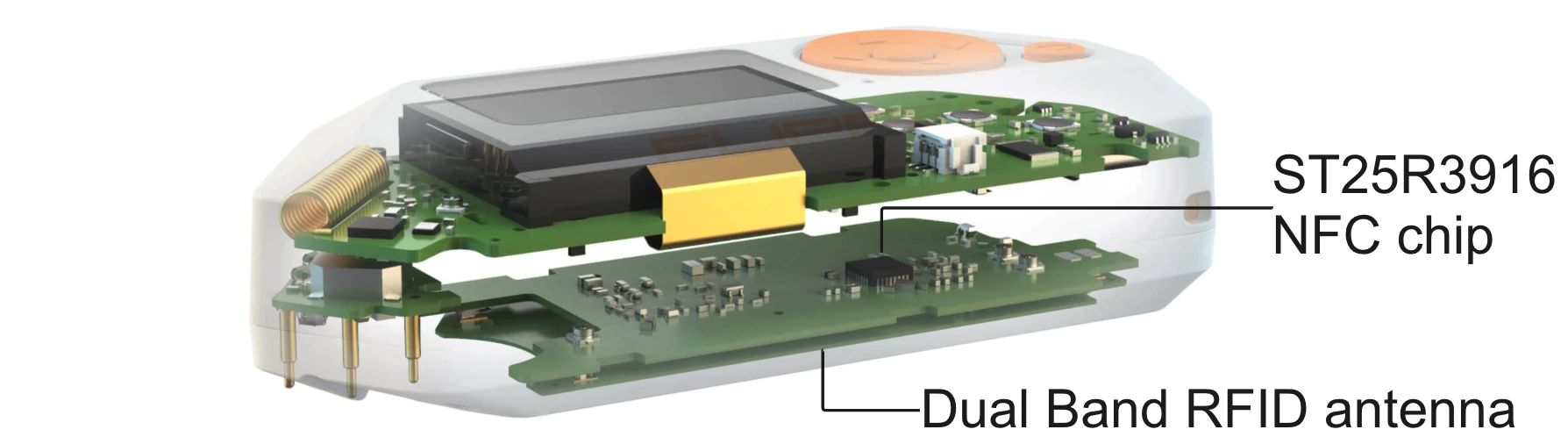
**Saved** — lists saved NFC cards, which can be emulated and renamed.

**Extra Actions** — additional reading scripts, plugins, keys management, and etc.

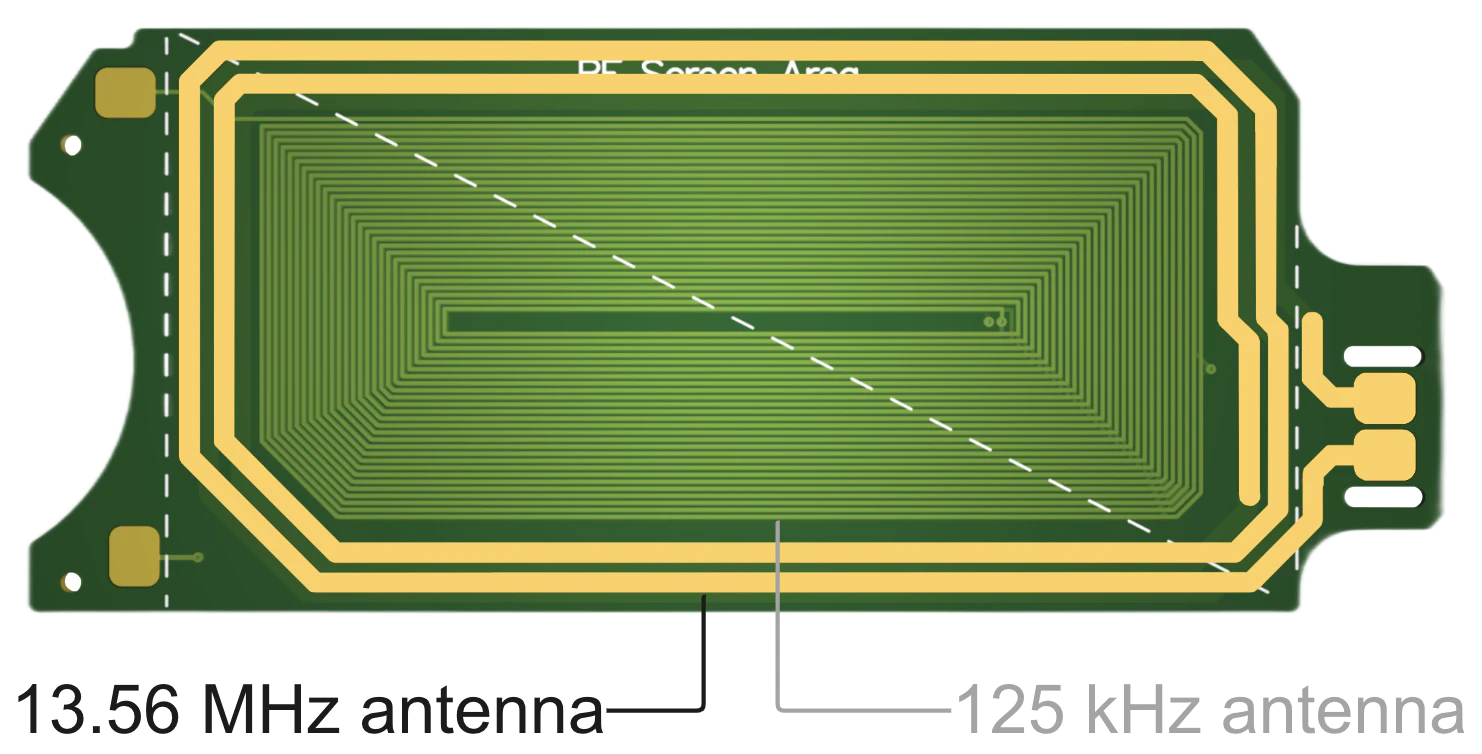
**Add Manually** — generates new virtual NFC cards by manually entering card's data.

## NFC hardware - See [NFC - Flipper Zero — Documentation](https://docs.flipperzero.one/nfc)

Flipper Zero has a built-in NFC module based on a [**ST25R3916 NFC chip**](https://www.st.com/en/nfc/st25r3916.html#overview) and a 13.56 MHz high-frequency antenna. The chip is used for high-frequency protocols and responsible for reading and emulation of cards.



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



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

# Extra - Flipper Zero

## 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)

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

# MIFARE IC

## History

First deployed in 1994, MIFARE ICs were originally developed for automated fare collection in public transport, but that was just the beginning. Since then, MIFARE enables contactless transit, payment, and access experiences for citizens, independent of location and time.

## Characteristic

By supporting true multi-application functionality, mobile formats, and offering certified Common Criteria security, MIFARE ICs combine convenience with efficiency. Choosing MIFARE products means choosing a solution that is already available in a widespread infrastructure, and that means reduced startup costs and greater scalability. MIFARE ICs can interact with Near Field Communication (NFC), and communicating through NFC means that MIFARE products can also be managed and implemented via NFC-enabled mobile devices, such as smartphones, watches, and more.