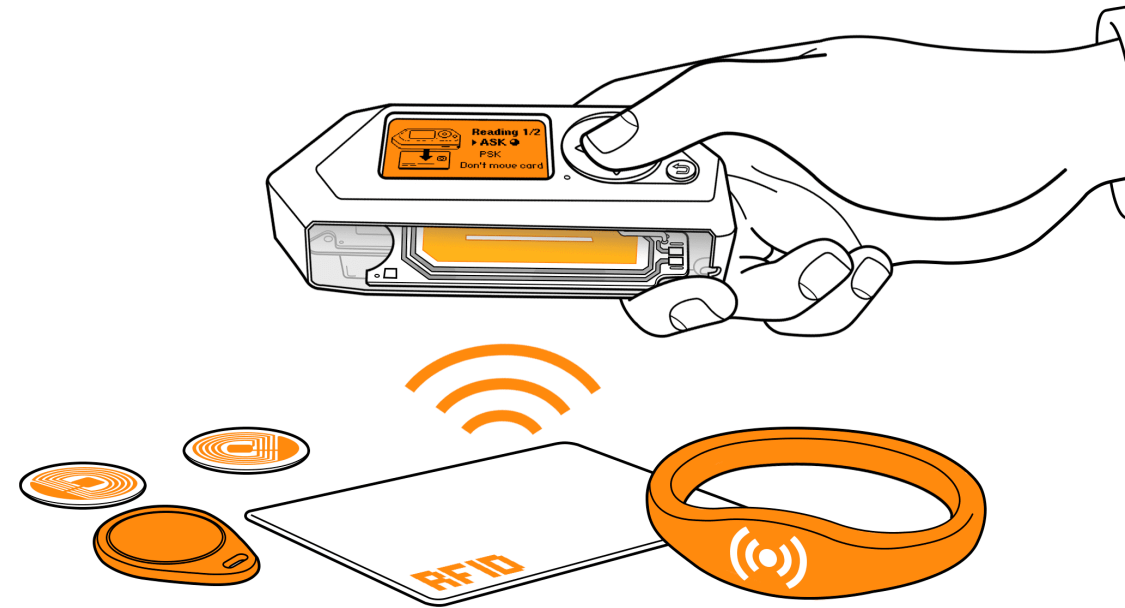


Flipper Zero: Hackujeme RFID 🐉



Představení

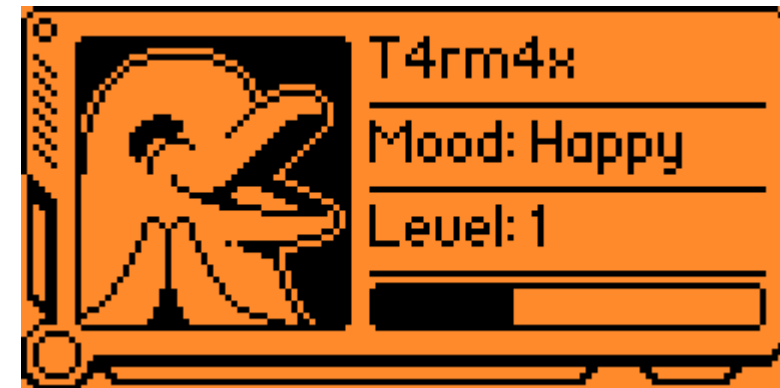


Adam

- Senior Engineer
@ [2Ntelecom](#)
- Cofounder and retired keeper
@ [bastlirna](#)

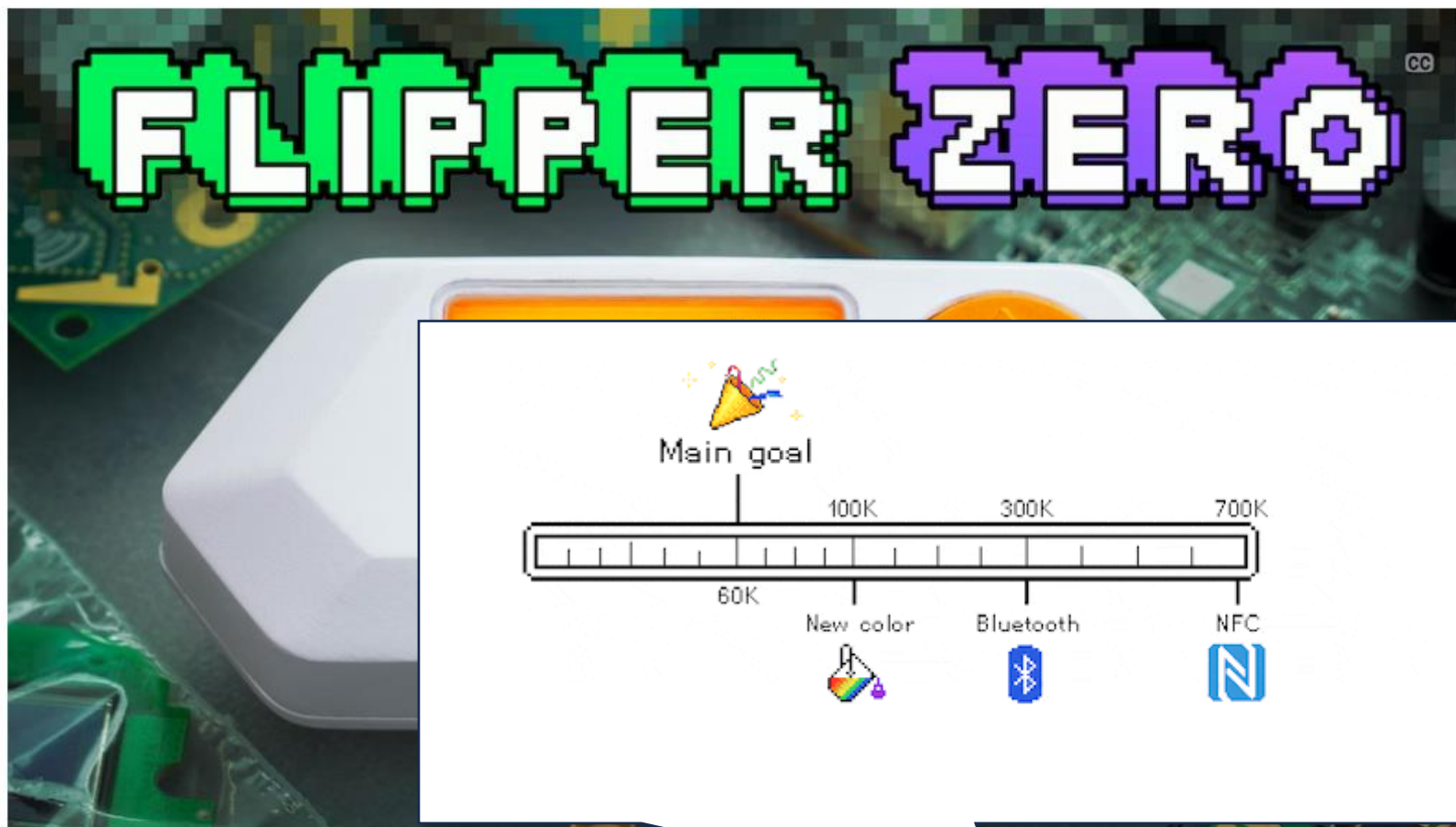


T4rm4x



MacGyver
macgyver.siliconhill.cz

2N



Flipper Zero — Multitool for Hackers

\$4,882,784

pledged of \$60,000 goal

Available rewards

1X Flipper Zero \$119

👉 — Early Bird

Save \$50

Limited Early Bird Price

Off Estimate Retail Price (\$169)

Payment will be charged via our
manager after the campaign.



Ships to

Anywhere in the
world

Free delivery

21

Limited quantity

52 left of 32974

Included

Flipper Zero, USB Type-C cable

[Details](#)

[Pledge US\\$ 119](#)

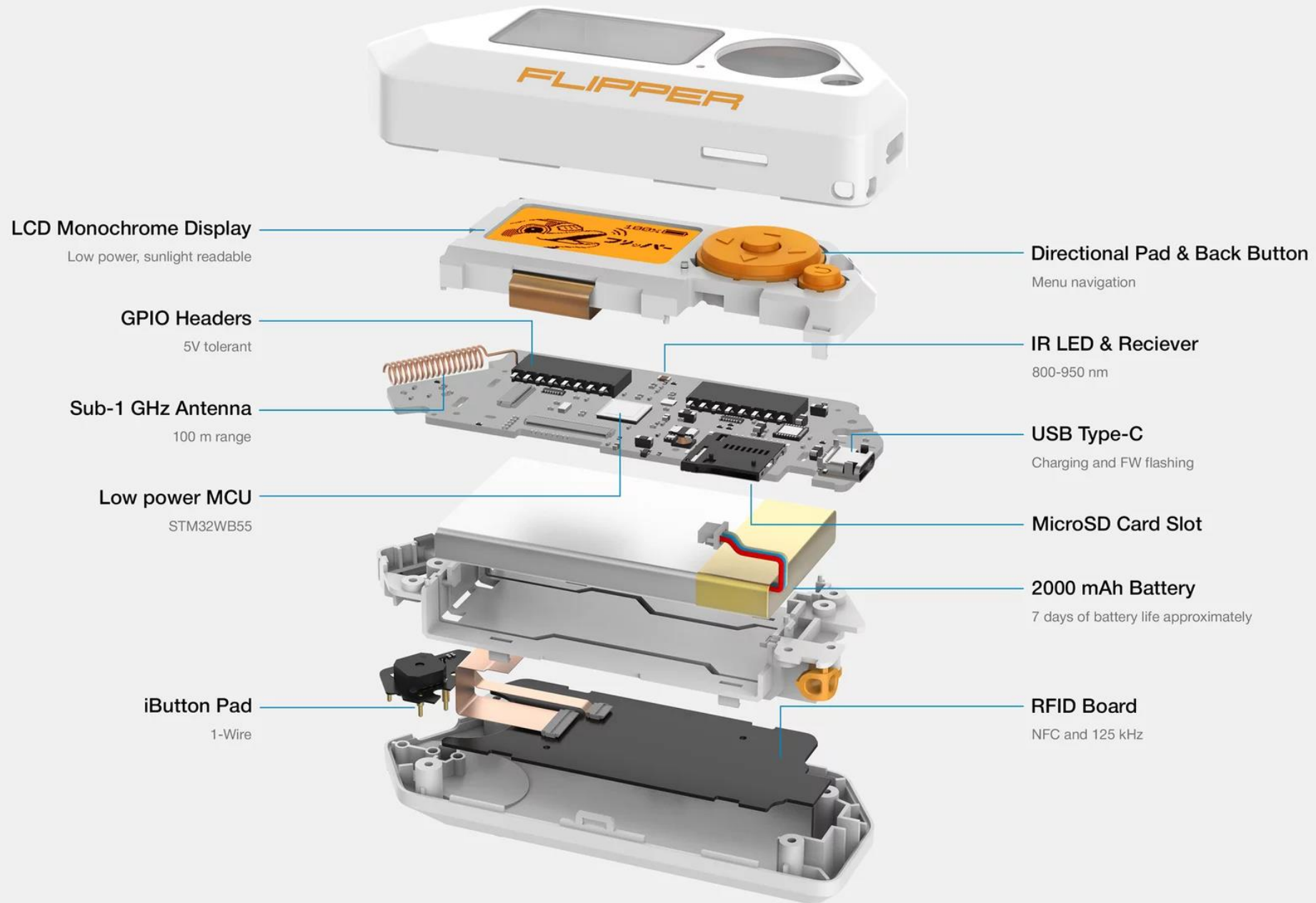
1X Flipper Zero — \$129

Kickstarter Special

KICKSTARTER (2020 — 2022)



FLIPPER ZERO IS A PORTABLE MULTI-TOOL FOR
PENTESTERS AND GEEKS IN A TOY-LIKE BODY



PÁR Z MNOHA PROJEKTŮ, NA KTERÝCH FLIPPER STOJÍ



YARD Stick One



TV B Gone



Hydra NFC

ne Display

night readable

D Headers

5V tolerant

Sub-1 GHz Antenna

100 m range

ower MCU

STM32WB55

Button Pad

1-Wire

Directional Pa

Menu navigation

IR LED & Reci

800-950 nm

USB Type-C

Charging and FW flashing

MicroSD Card

2000 mAh Bat

7 days of battery life

RFID Board

NFC and 125 kHz



Proxmark



USB Rubber Ducky

Science

[SILICON VALLEY](#) · [YOUTUBE](#) · [GOOGLE](#) · [LATEST NEWS](#)

TIKTOK TRENDS >

Flipper Zero: The 'tamagotchi for hackers' goes viral on TikTok

Dozens of users have been sharing videos using the device to turn on the television and unlock cars and hotel rooms





[Home](#) > [News](#) > [Technology](#) > [Flipper Zero banned by Amazon for being a 'card skimming device'](#)

Flipper Zero banned by Amazon for being a 'card skimming device'

By [Sergiu Gatlan](#)

 April 7, 2023

 05:01 AM

 0





[Flipper Zero/Facebook](#)

EXCLUSIVE: Hacking tool Flipper Zero tracked by intelligence agencies, which fear white nationalists may deploy it against power grid

'Racially and ethnically motivated violent extremists may seek to exploit the hacking capabilities of a new cyber penetration tester.'



Which One is More Dangerous??



8.2K views • 1 month ago

<https://youtu.be/1OXGrRe5Sak?si=Q9rbysC32RIVUkyv>



Pozor na toto zařízení - Flipper zero



Killeroz

43.5K subscribers

Join



Subscribed ▼

801



Share

Download



32K views 6 months ago

https://youtu.be/wv8t8fnm4QY?si=wbzPYSgvN_NVgk1h

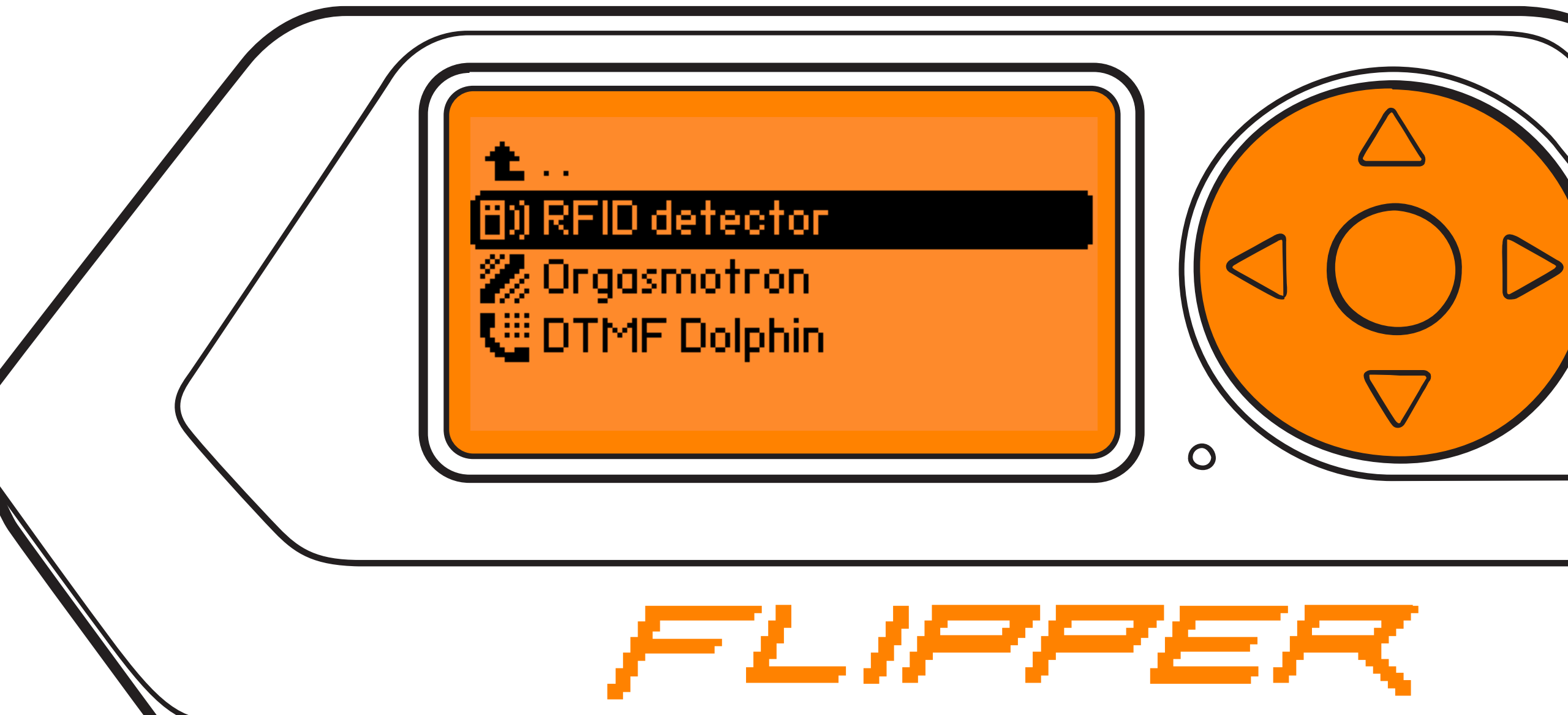
...run. Video není natočeno za účelem někoho nabádat k stejným
...ové zařízení existuje a například lépe zabezpečili svá data. Já

O čem se budeme bavit

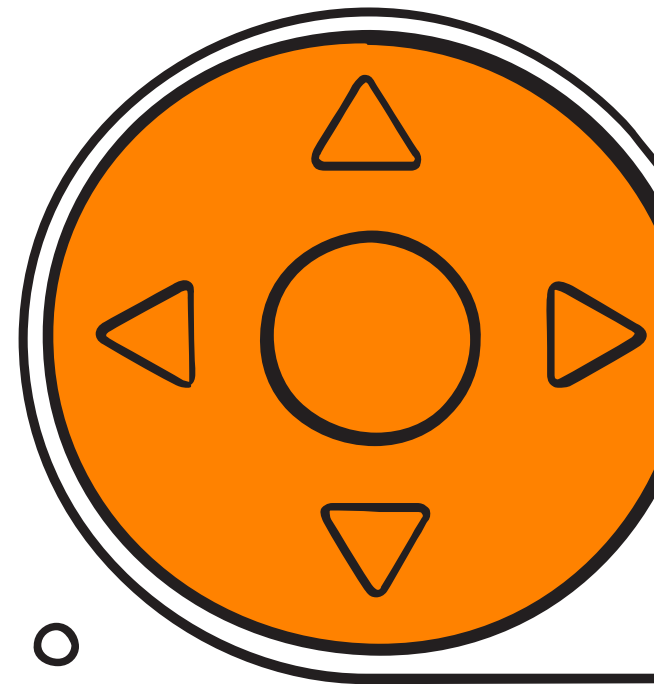
- RFID a NFC schopnosti Flippera
- Primárně ACS (přístupové systémy)
- Use-case **kopírování karet** (přečtení a emulace karty)
- 125 kHz (LF) a 13.56 MHz (HF)

RFID DETECTOR

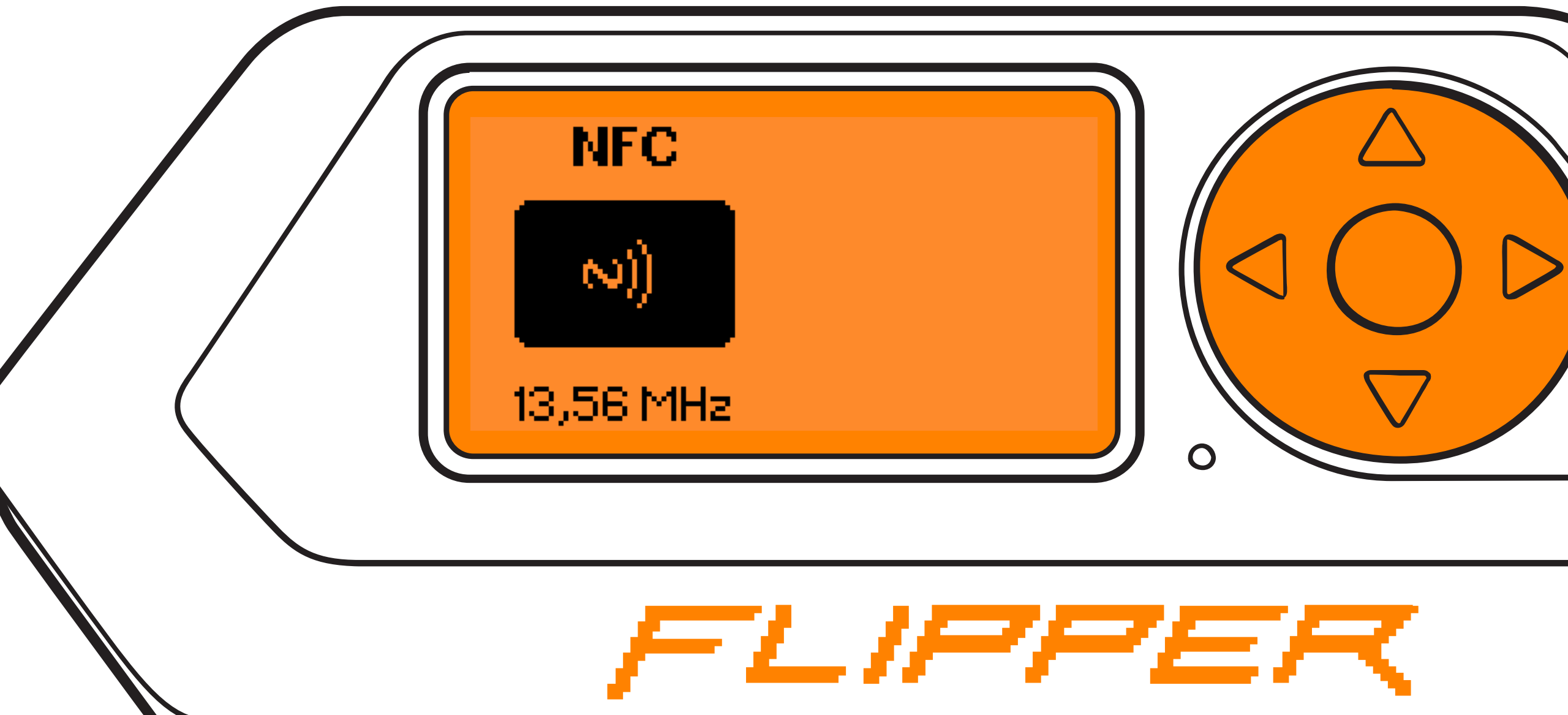
Aplikace pro detekci LF nebo HF pole



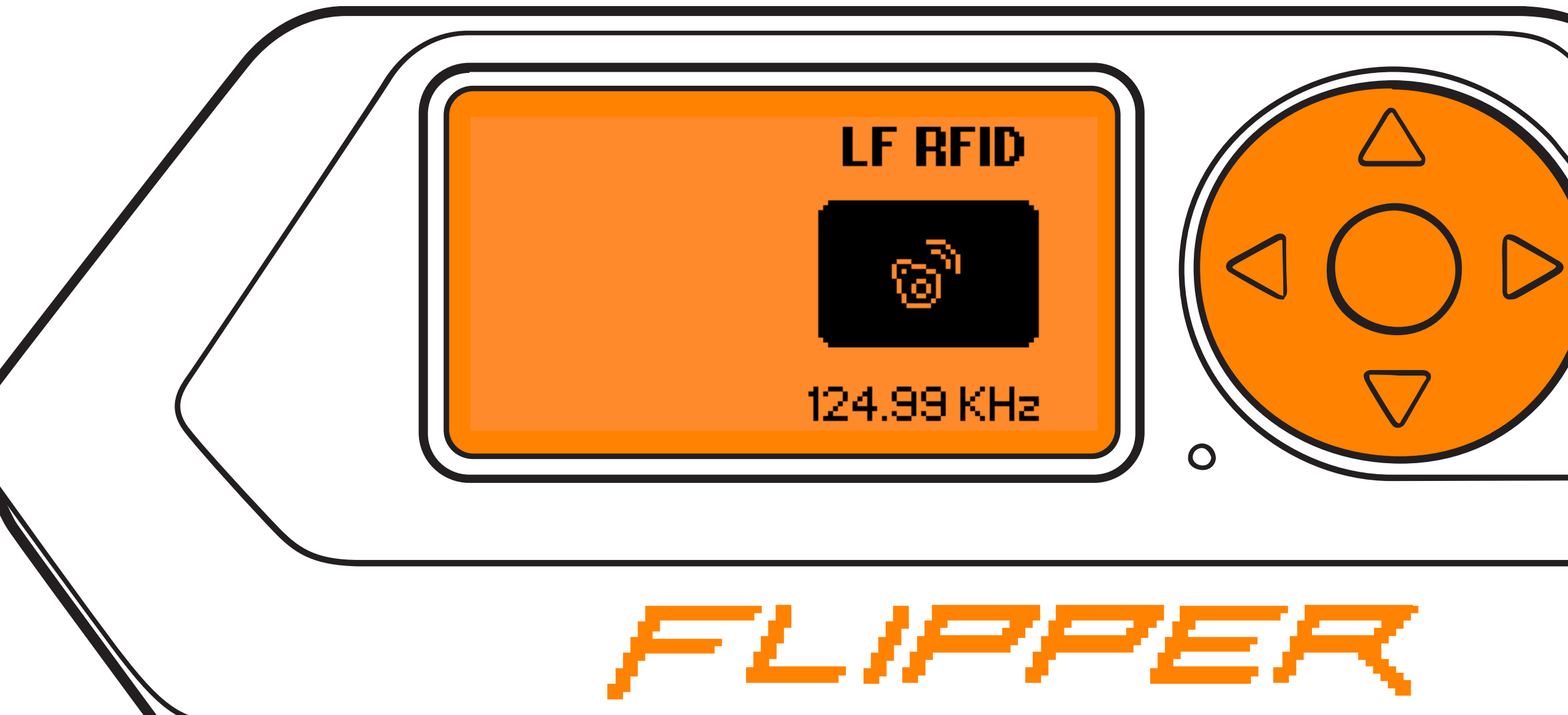
FLAPPER



FLAPPER



FLAPPER



FLAPPER

125 KHZ RFID

EM4100

- EM Microelectronic
- ~1990
- Velmi rozšířené (aspoň u nás)

System Principle

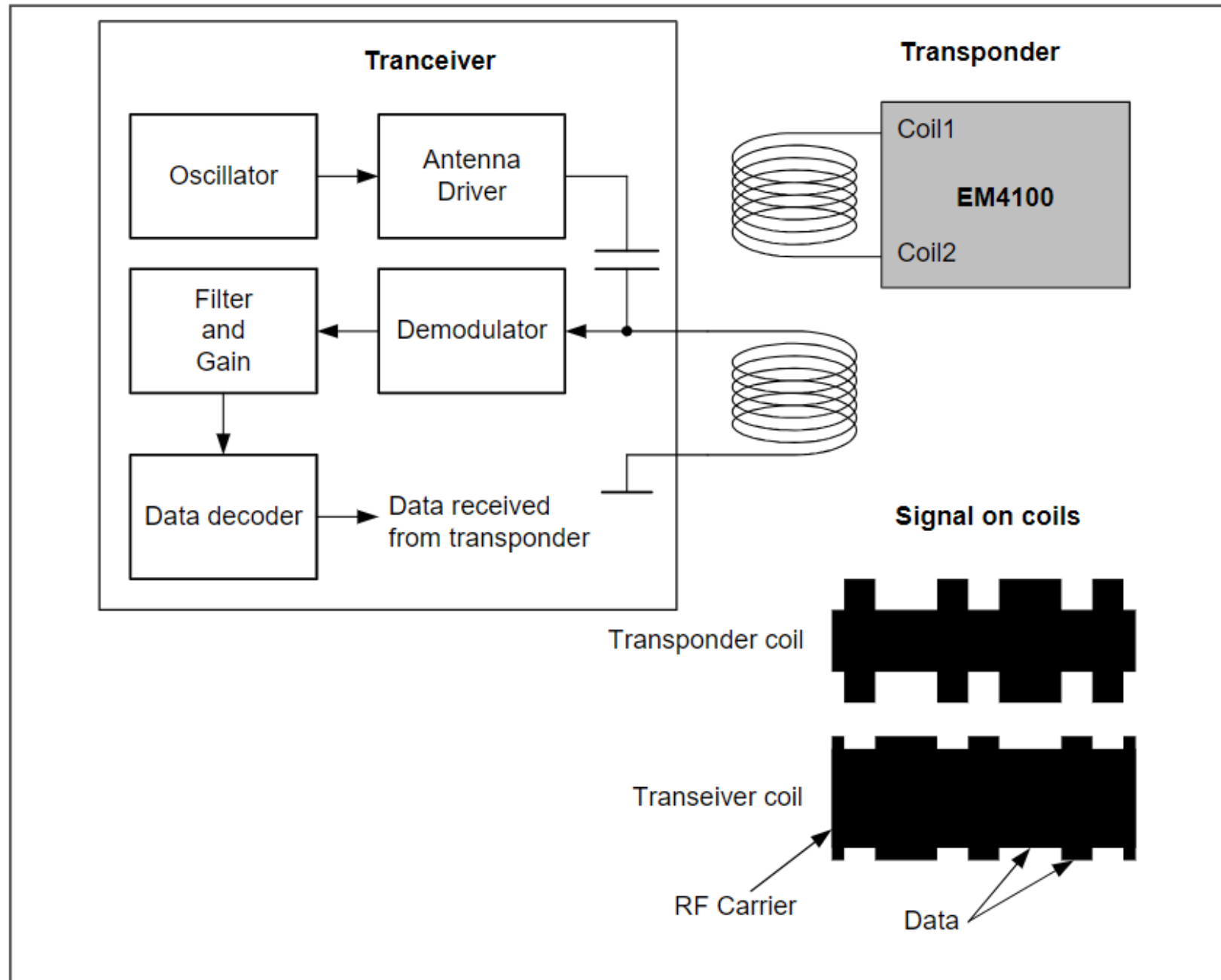
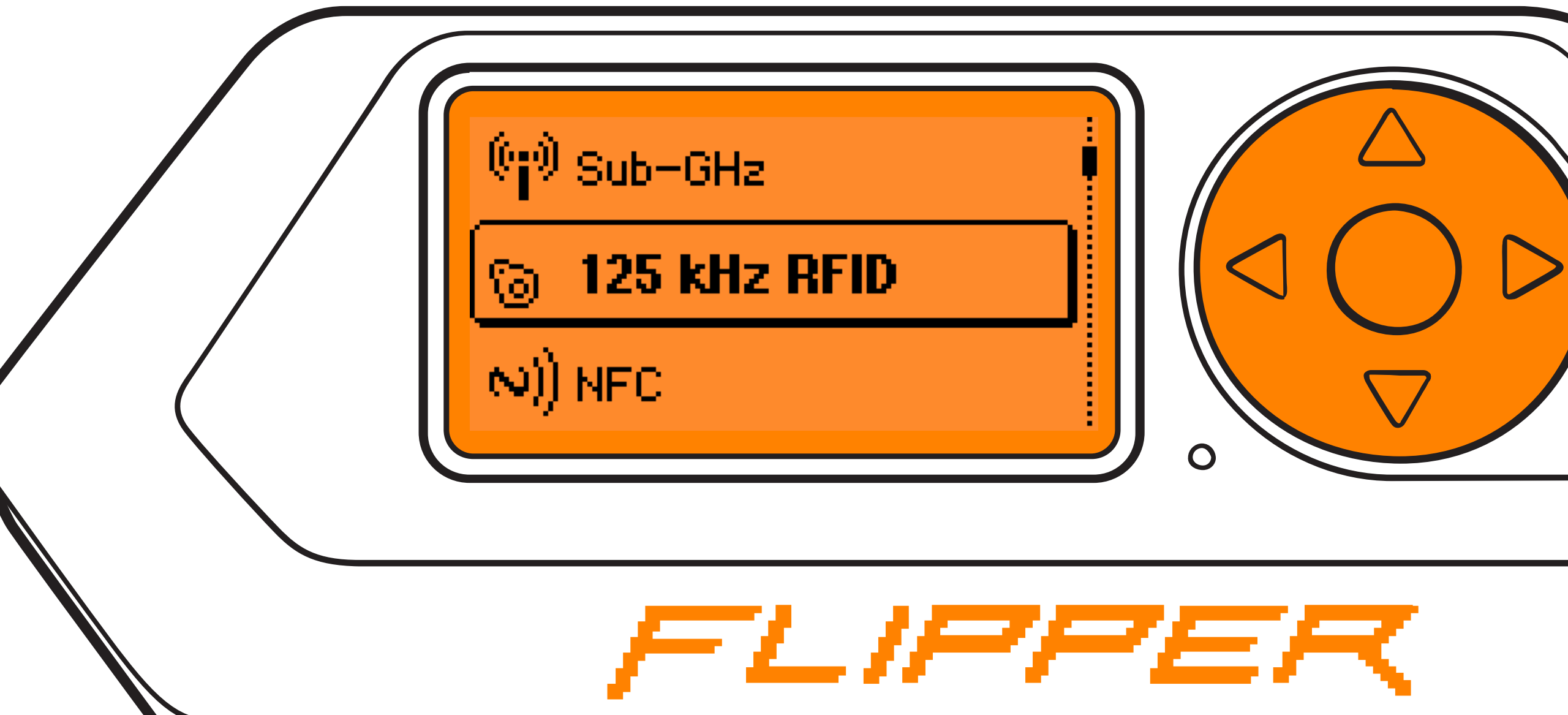
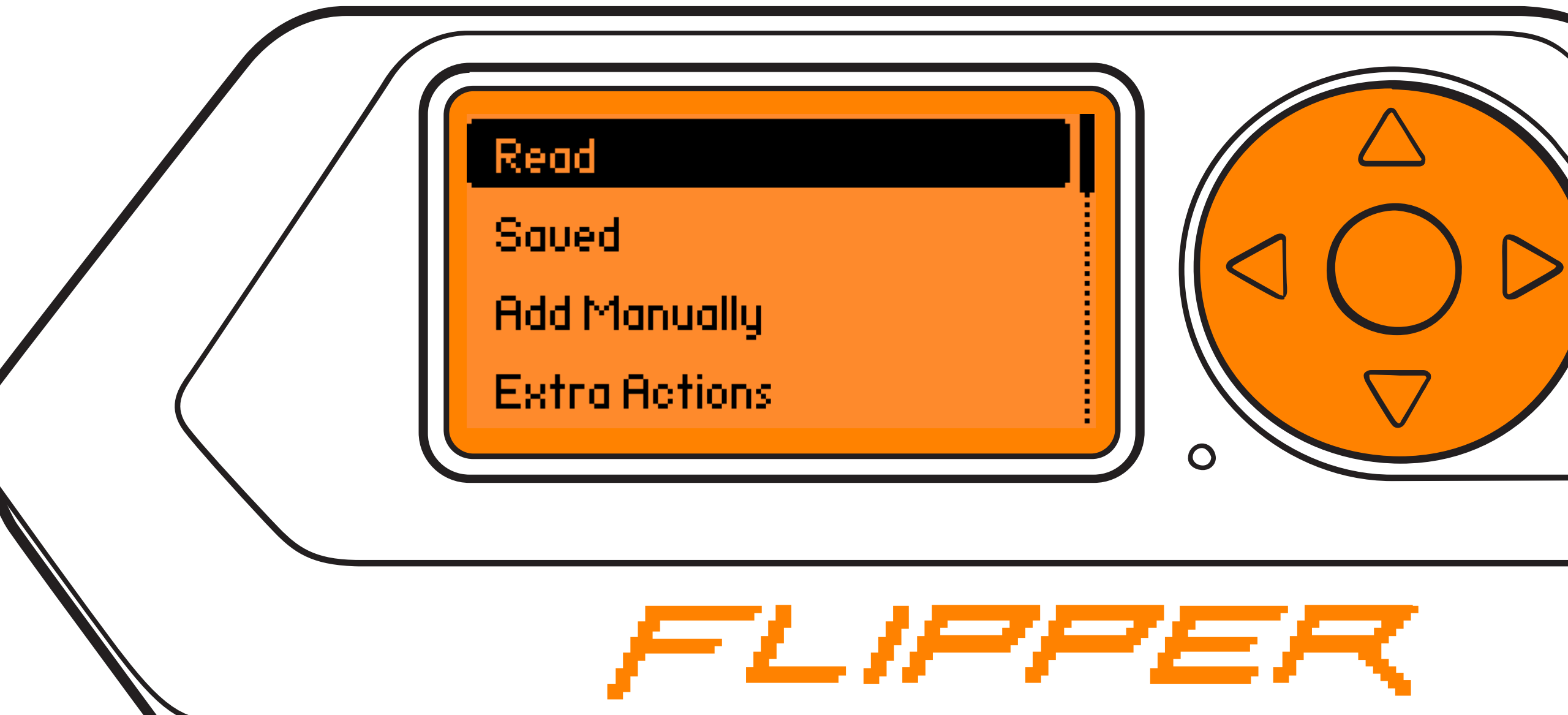


Fig. 3



FLAPPER



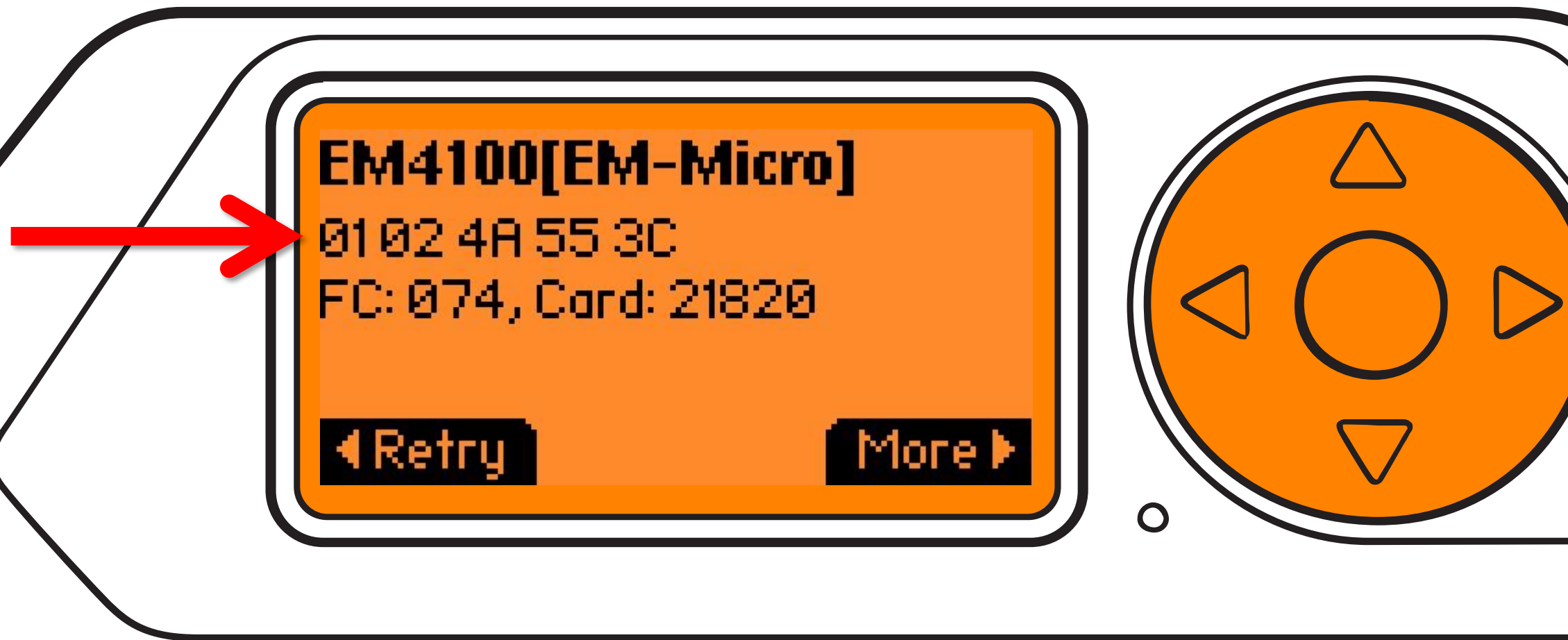
Read

Saved

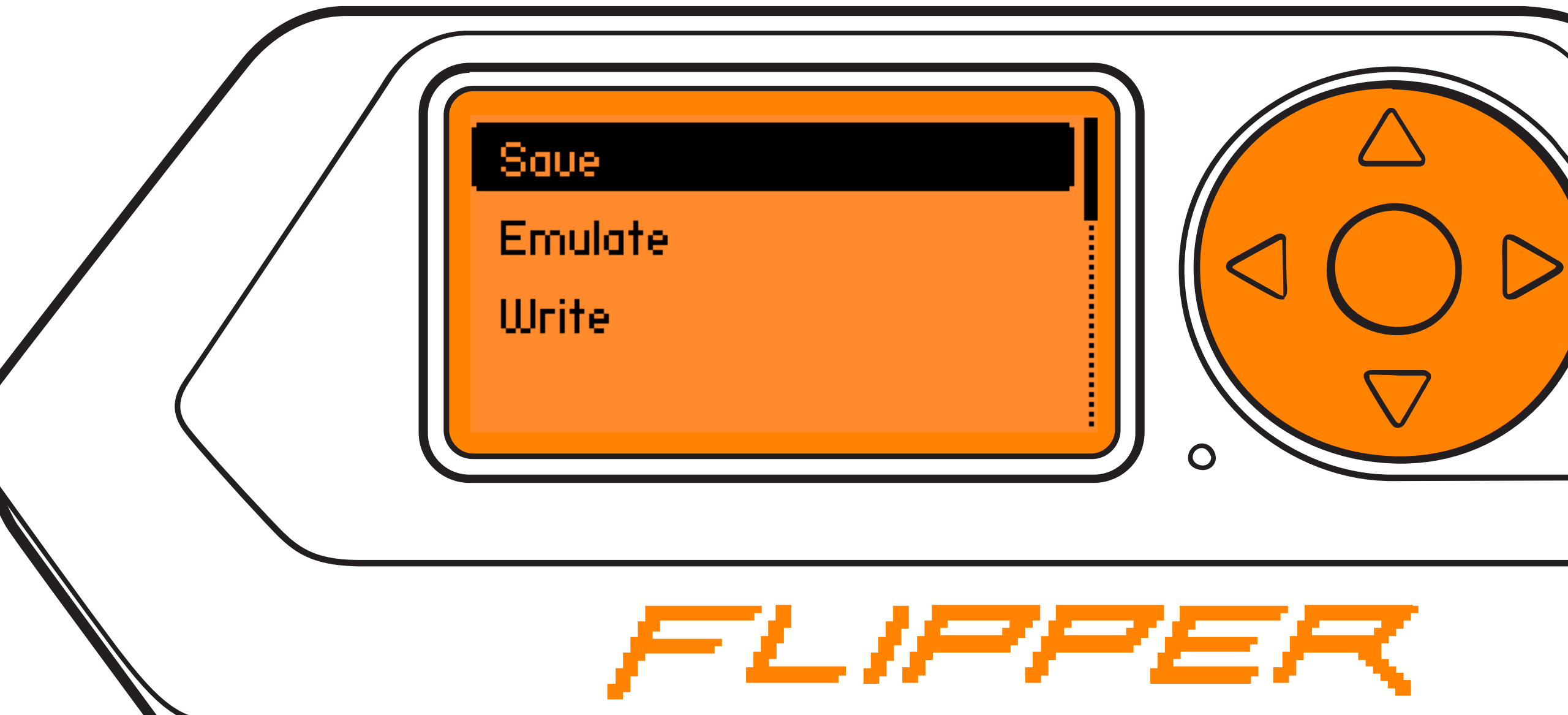
Add Manually

Extra Actions

FLAPPER



FLAPPER

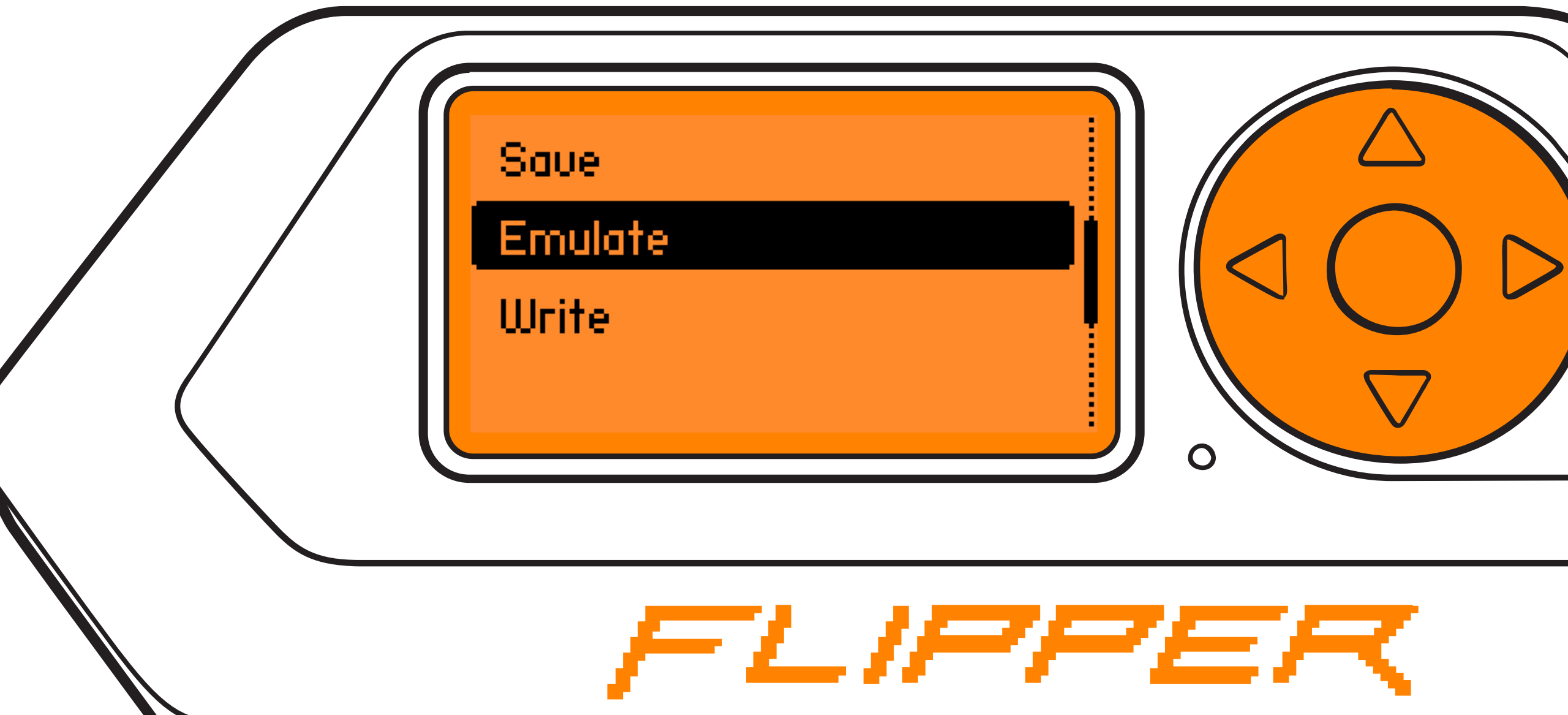


Save

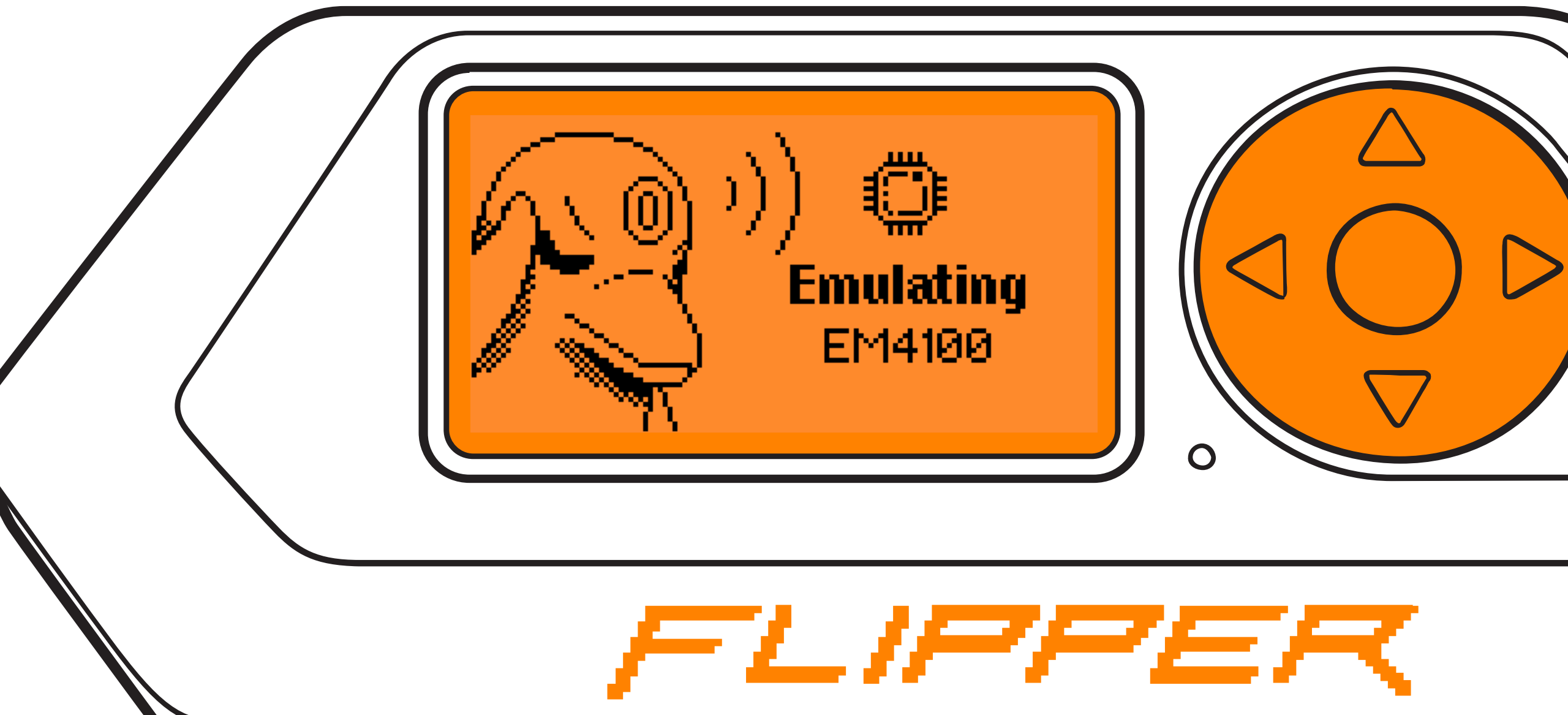
Emulate

Write

FLAPPER



FLAPPER



FLAPPER

Generating 125 kHz RFID cards

You can manually generate virtual cards with the following protocols:

- EM-Micro EM4100
- HID H10301
- IDTECK Idteck
- Motorola Indala 26
- Kantech IoProx XSF
- AWID
- FECAVA FDX-A
- ISO FDX-B
- Generic HID Prox
- Generic HID Ext
- Farpointe Pyramid
- Viking
- Jablotron
- Paradox
- PAC Stanley
- Keri
- Gallagher
- Honeywell Nexwatch

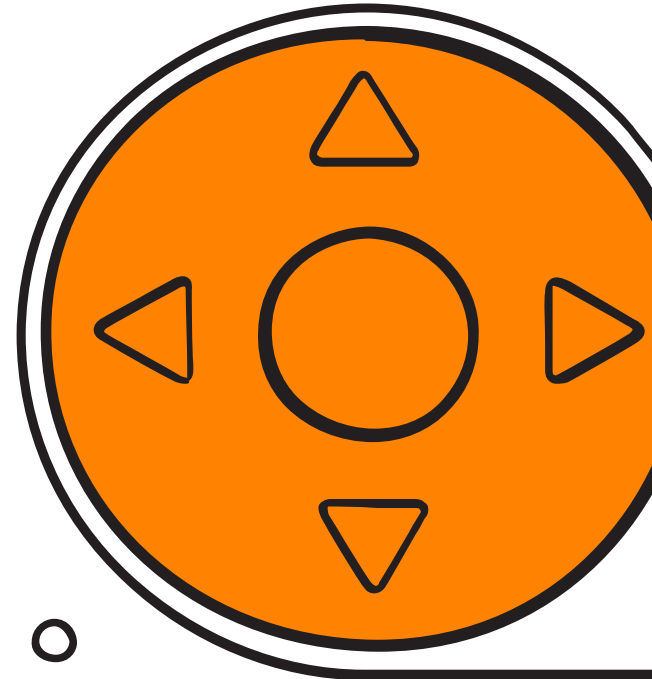
Jablotron[Jablotron]

00 00 61 42 30

ID: 95F56

◀ Retry

More ▶



FLAPPER

Závěr EM4100

- Jednosměrná komunikace
- Naprosto žádné zabezpečení proti kopírování
- Je to ~30 let stará technologie → v té době nikdo neřešil bezpečnost

JAK TO VYLEPŠIT? 🤔

13.56 MHZ RFID

MIFARE Classic

- Philips (NXP)
- ~ 1995 - 2000
- Komunikace podle ISO14443A

ISO14443A

- ~ TCP (1 – 5 vrstva z OSI/ISO modelu)
- Definuje jak komunikovat
- Neřeší zabezpečení komunikace (to jo o úroveň výše)
- PICC (karta) musí mít ID (~ MAC adresa)
- ID je často unikátní (UID)



ANT V6.2
Center Freq: 13.56MHz
PROG: 21ND

[+] Recorded activity (trace len = 77 bytes)

[=] start = start of start frame end = end of frame. src = source of transfer

[=] ISO14443A - all times are in carrier periods (1/13.56MHz)

Start	End	Src	Data (! denotes parity error)	CRC	Annotation
0	992	Rdr	52(7)		WUPA
2100	4468	Tag	04 00		
7040	9504	Rdr	93 20		ANTICOLL
10548	16436	Tag	70 49 ab 28 ba		
19072	29600	Rdr	93 70 70 49 ab 28 ba e8 f2	ok	SELECT_UID
30644	34164	Tag	08 b6 dd	ok	



Read

Detect Reader

Saved

Extra Actions

FLAPPER

Mifare Classic 1K

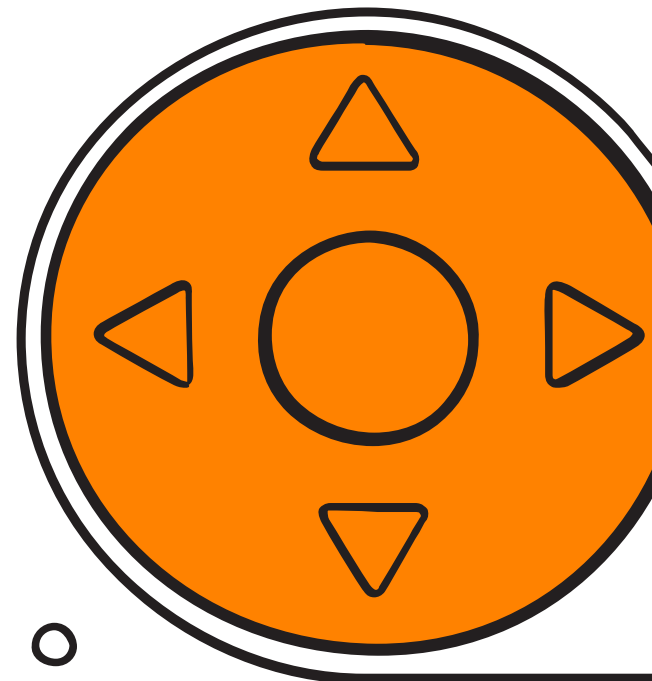
UID: 70 49 AB 28

Keys Found: 32/32

Sectors Read: 16/16

◀ Retry

More ▶



FLAPPER

Závěr ISO14443A (ID)

- Oproti EM4100 obousměrná a rychlá komunikace
- Žádné zabezpečení proti kopírování
- UID nemusí být unikátní (většinou je ale unikátní *enough*)
- ~ HTTP



JAK TO VYLEPŠIT? 🤔

MIFARE Ultralight

- ISO14443A karta
- Super levná
- Až 164B uživatelské paměti
- Čtení/zápis může být chráněn 32bit heslem
- Počet pokusů o autentizaci může být omezen (zablokování karty)
- Podobných karet je víc, např. **STM ST25TA02KB**

IKEA ROTHULT





[+] Recorded activity (trace len = 850 bytes)
[=] start = start of start frame end = end of frame. src = source of transfer
[=] ISO14443A - all times are in carrier periods (1/13.56MHz)

Start	End	Src	Data (! denotes parity error)	CRC	Annotation
0	1056	Rdr	26(7)		REQA
2244	4612	Tag	42 00		
29568	34336	Rdr	50 00 57 cd	ok	HALT
107312	108304	Rdr	52(7)		WUPA
109572	111940	Tag	42 00		
140432	142896	Rdr	93 20		ANTICOLL
144084	149972	Tag	88 02 e3 01 68		
176016	186544	Rdr	93 70 88 02 e3 01 68 cc 20	ok	SELECT_UID
187716	191236	Tag	04 da 17		
216768	219232	Rdr	95 20		ANTICOLL-2
220420	226308	Tag	19 e2 1f fb 1f		
252400	262864	Rdr	95 70 19 e2 1f fb 1f 0d 56	ok	SELECT_UID-2
264116	267700	Tag	20 fc 70		
289952	294720	Rdr	50 00 57 cd	ok	HALT
367728	368784	Rdr	26(7)		REQA
2420896	2421952	Rdr	26(7)		REQA
2423124	2425492	Tag	42 00		
2450464	2455232	Rdr	50 00 57 cd	ok	HALT
2528208	2529200	Rdr	52(7)		WUPA
2530468	2532836	Tag	42 00		
2561312	2563776	Rdr	93 20		ANTICOLL
2564964	2570852	Tag	88 02 e3 01 68		
2596896	2607424	Rdr	93 70 88 02 e3 01 68 cc 20	ok	SELECT_UID
2608612	2612132	Tag	04 da 17		
2637648	2640112	Rdr	95 20		ANTICOLL-2
2641300	2647188	Tag	19 e2 1f fb 1f		
2673280	2683744	Rdr	95 70 19 e2 1f fb 1f 0d 56	ok	SELECT_UID-2
2684996	2688580	Tag	20 fc 70		
2710848	2715616	Rdr	50 00 57 cd	ok	HALT
2788608	2789664	Rdr	26(7)		REQA
4179072	4180128	Rdr	26(7)		REQA
4181332	4183700	Tag	42 00		
4208656	4213424	Rdr	50 00 57 cd	ok	HALT
4287216	4288208	Rdr	52(7)		WUPA
4289460	4291828	Tag	42 00		
4320240	4322704	Rdr	93 20		ANTICOLL
4323892	4329780	Tag	88 02 e3 01 68		
4355808	4366336	Rdr	93 70 88 02 e3 01 68 cc 20	ok	SELECT_UID
4367540	4371060	Tag	04 da 17		
4396400	4398864	Rdr	95 20		ANTICOLL-2
4400036	4405924	Tag	19 e2 1f fb 1f		
4432016	4442480	Rdr	95 70 19 e2 1f fb 1f 0d 56	ok	SELECT_UID-2
4443748	4447332	Tag	20 fc 70		
4469616	4474384	Rdr	e0 80 31 73	ok	RATS
4475556	4483748	Tag	05 75 80 60 02 bb 58	ok	
4506672	4512528	Rdr	d0 11 00 52 a6	ok	PPS
4513780	4517300	Tag	d0 73 87		
4541264	4559792	Rdr	02 00 a4 04 00 07 d2 76 00 00 85 01 01 00 35 c0	ok	
4561812	4567636	Tag	02 90 00 f1 09		
4591072	4602752	Rdr	03 00 a4 00 0c 02 00 01 81 7c	ok	
4604196	4610020	Tag	03 90 00 2d 53		
4633104	4642416	Rdr	02 00 20 00 01 00 6e a9	ok	
4643684	4649508	Tag	02 63 00 91 5f		
4675152	4702960	Rdr	03 00 20 00 01 10 c7 e0 64 62 d0 03 c7 67 53 51 e3 9f		
			03 83 fd 4a f0 e3	ok	
4706308	4712132	Tag	03 90 00 2d 53		
4735232	4744544	Rdr	02 a2 b0 00 00 1d 51 69	ok	
4750004	4789236	Tag	02 00 1b d1 01 17 54 02 7a 68 05 93 a1 f0 3b 7a 05 28		
			6d bc 34 2d 15 ec 0e 8a 31 31 31 32 90 00 59 95	ok	

[illegible]

2132	Tag	04	da	17																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																</
------	-----	----	----	----	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	----

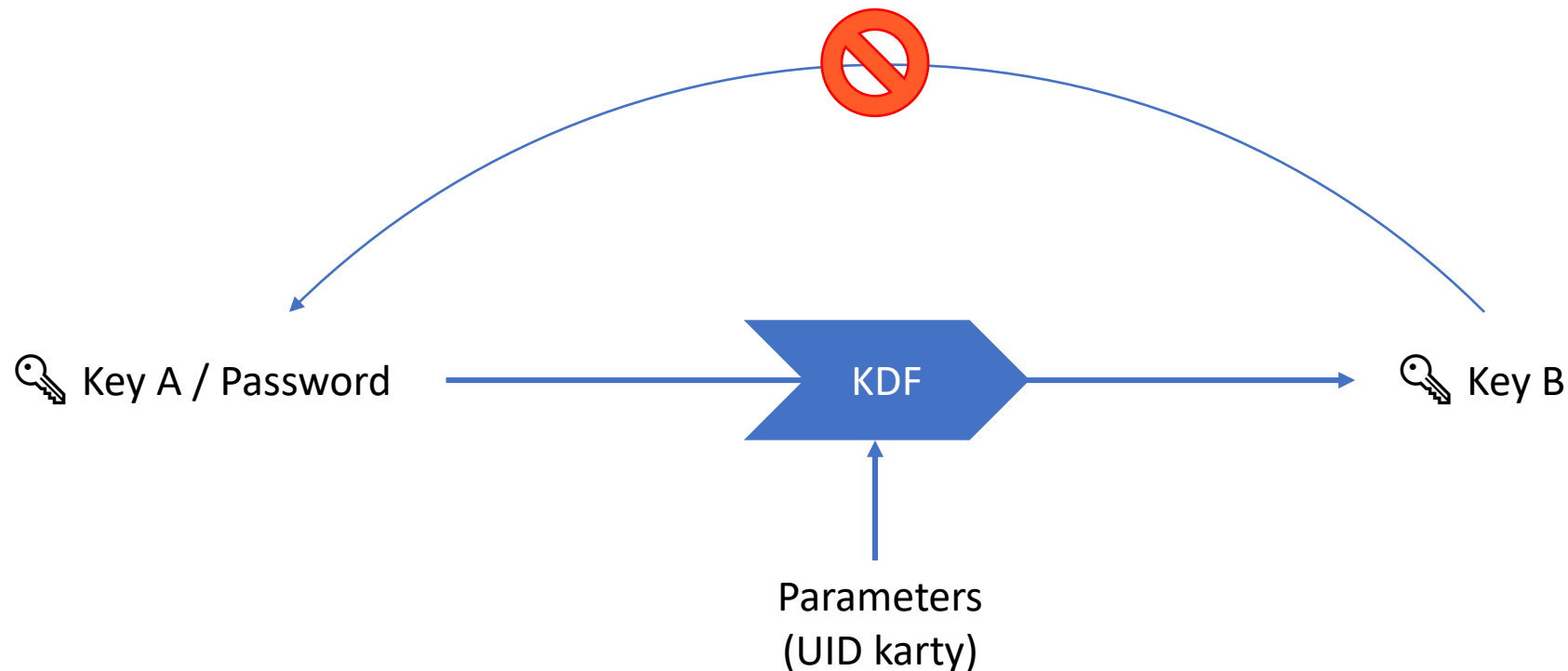
Jak zjistit heslo?

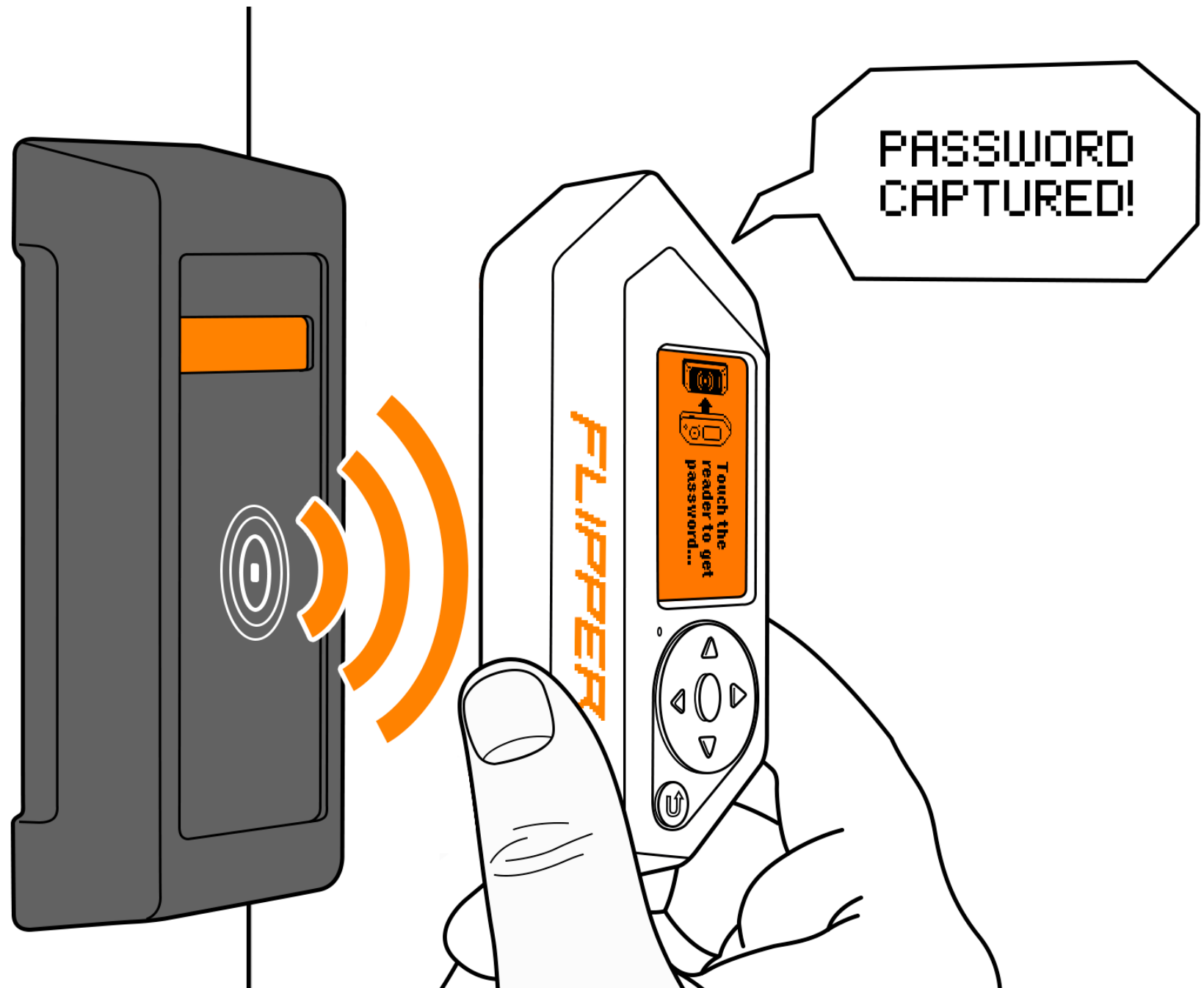
- MITM se dělá blbě, aby o tom majitel karty nevěděl 😞
- Slovní útok nebo útok hrubou silou může kartu zablokovat
- Flipper může předstírat, že je karta a počkat až mu čtečka pošle heslo
- Ale... mají všechny karty stejné heslo? 🤔

Key derivation function

Key derivation function (KDF) is a cryptographic algorithm that derives secret key from a secret value such as a main key, a password, or a passphrase.

-- Wikipedia





PASSWORD
CAPTURED!

FLIPPER

Touch the
reader to get
password...

Závěr MF Ultralight

- Autentizace už není na základě ID karty
- Ale na základě uživatelských dat (můžou být např. podepsaná, ...)
- Data jsou chráněna heslem
 - *To je dobrý*
- Heslo je přenášeno v plaintextu
 - *To je špatný*
- ~ HTTP Basic Authentication (po HTTP)

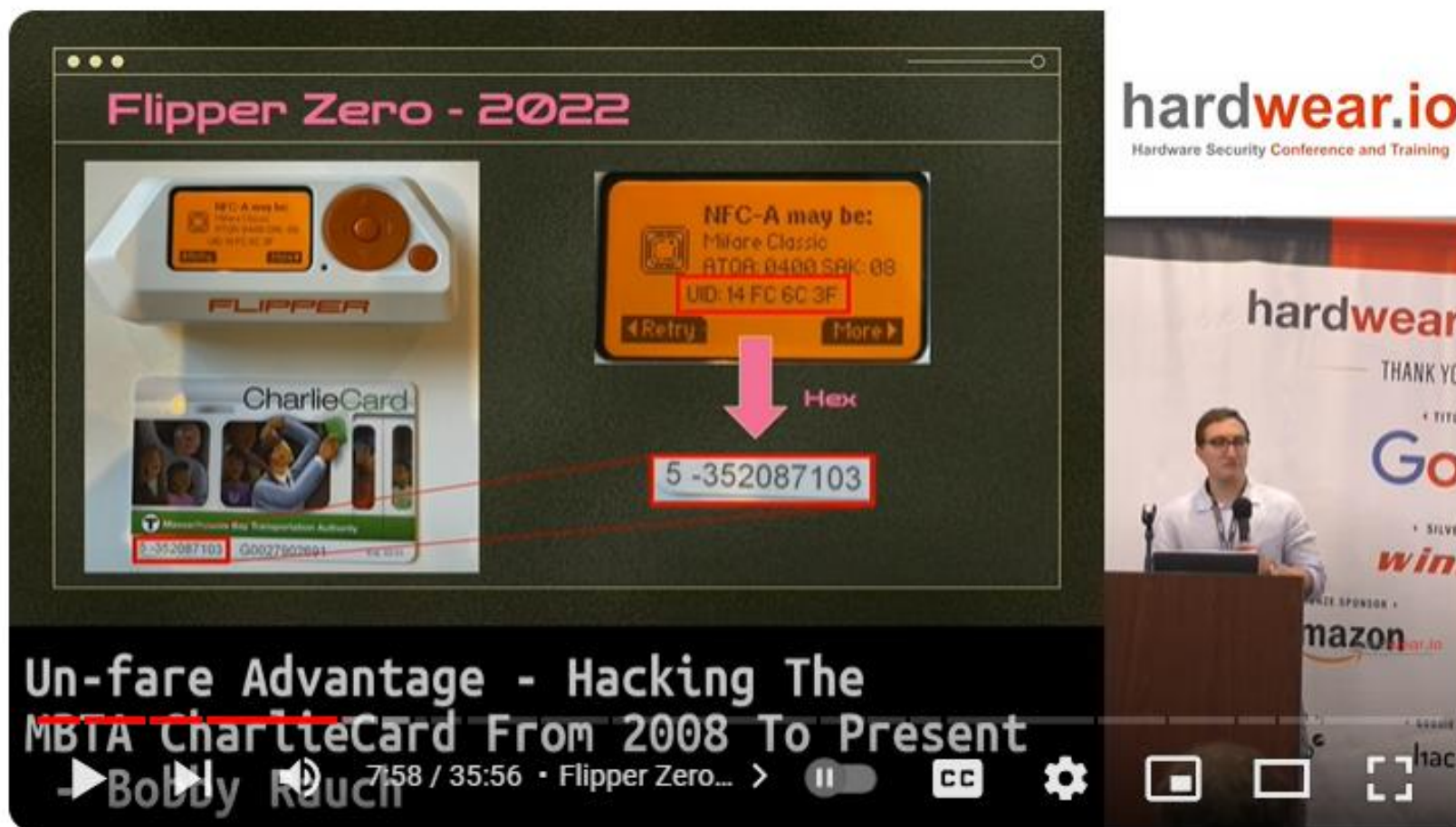
JAK TO VYLEPŠIT? 🤔

MF Classic

- ISO14443A karta
- Super stará (= častá a levná)
- 1kB nebo 4kB uživatelské paměti
- Rozděleno do sektorů
- Každý sektor může mít dvě hesla (konfigurovatelné)
- Šifrovaná komunikace (Crypto1)
- Děravá jak cedník (...již od roku 2008)

Slovníkový útok

- MFC nemá omezený počet neuspěšných pokusů
- https://github.com/flipperdevices/flipperzero-firmware/blob/dev/assets/resources/nfc/assets/mf_classic_dict.nfc
- Aktuálně ~ 1500 klíčů
- Když znáte alespoň jeden klíč, jde snadněji zjistit ostatní (další ze zranitelností MFC)
- Existuje MFC EV1



"Un-fare Advantage" - Hacking The MBTA CharlieCard From 2008 To Present by Bobby Rauch | hardwear.io



hardwear.io
5.08K...



Subscribed



44



Share



<https://youtu.be/me6FyrDRID4?si=mKSdl2rFydNbnGh9>



Read

Detect Reader

Saved

Extra Actions

FLAPPER

MFkey32

- Útok přímo na Crypto 1
 - <https://www.cs.bham.ac.uk/~garciaf/publications/Dismantling.Mifare.pdf>
- Pokud máte dostatek nonce (začátek komunikace s kartou)
- Jde dopočítat klíč
- Je výpočetně náročnější



Závěr MF Classic

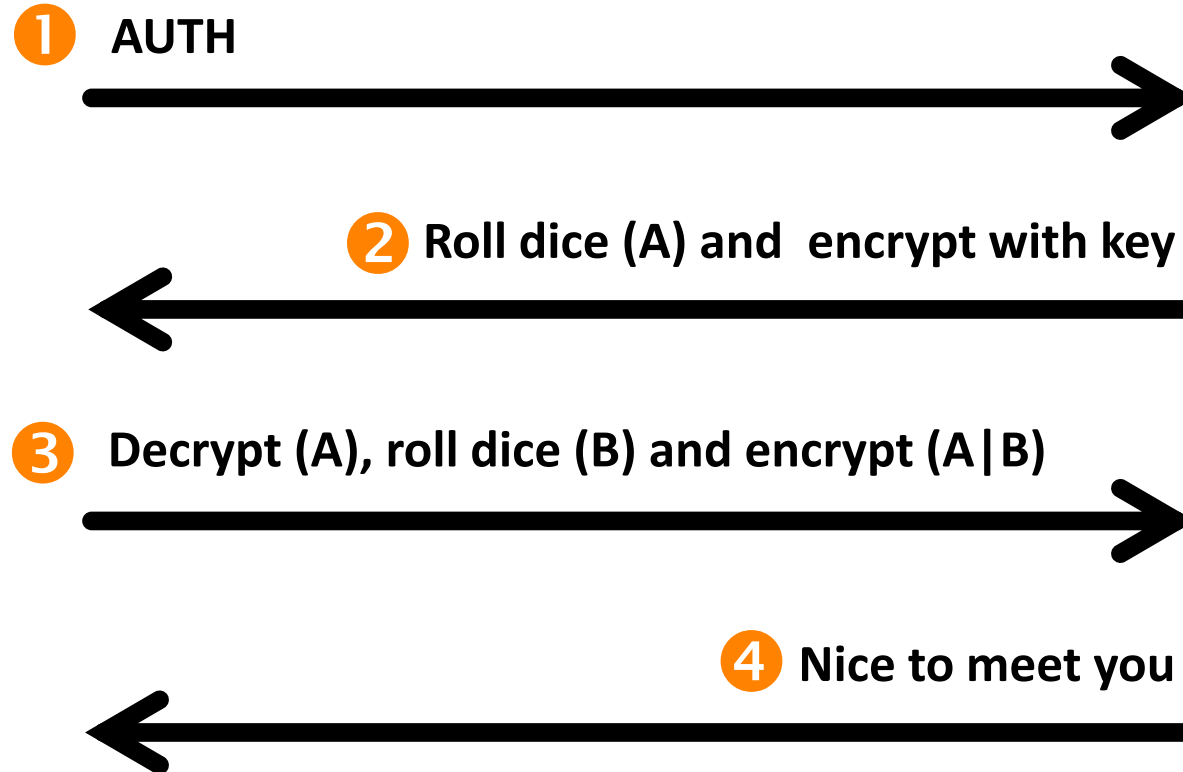
- Komunikace je šifrovaná
 - *To je dobrý*
- Home-brew (proprietární) crypto
 - *To je špatný*

JAK TO VYLEPŠIT? 🤔

MIFARE DESFire

- ISO14443A-4 karta
- Aktuální je EV3 (4. generace)
- AES-128
- Autentizaci i šifrování komunikace
- Plný datasheet pod NDA 🙊

Mutual authentication



Závěr DESFire

- Komunikace je šifrovaná
- Čtečka ani karta neodešlou nikdy heslo v čitelné podobě
- Standartní šifrovací algoritmus (AES)
- Symetrická kryptografie

JAK TO VYLEPŠIT? 🤔

FIDO

- FIDO norma podporuje mimo USB i NFC
- Asymetrická kryptografie
- Token umí podepsat challenge privátním klíčem
- ACS zná veřejný klíč a ověří tak majitele
- PIV, JCOB, ...



ZÁVĚR

Závěr

- Flipper není magická hůlka na každé dveře
- Snadno použitelný je na staré nebo dávno děravé technologie
- Umí toho mnohem víc (např. downgrade attack na HID) ale už to není typu „kliknu v menu“
 - Note: cena útoku s čase klesá
- Tam, kde na tom záleží používejte aktuální technologie

**So my neighbor put a
lock on their fence...**



Otázky?

@horcicaa

adam@horcica.cz

MacGyver
macgyver.siliconhill.cz