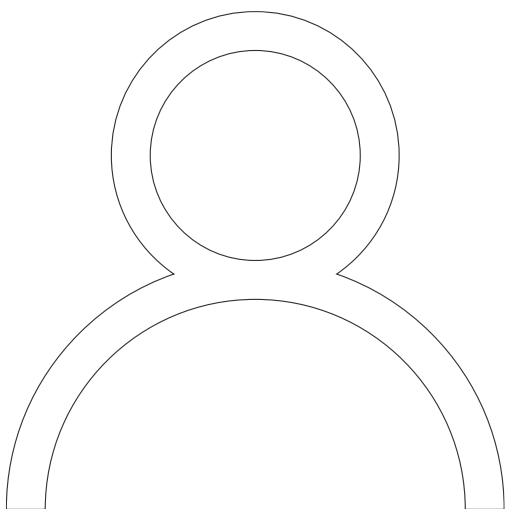
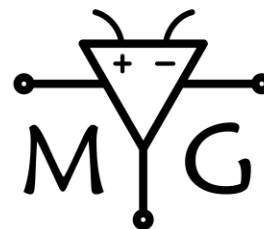


Adam Hořčica

@horcicaa



- Senior Engineer
[2N Telekomunikace a.s.](#)
- Cofounder and retired keeper
[@bastlirna](#)

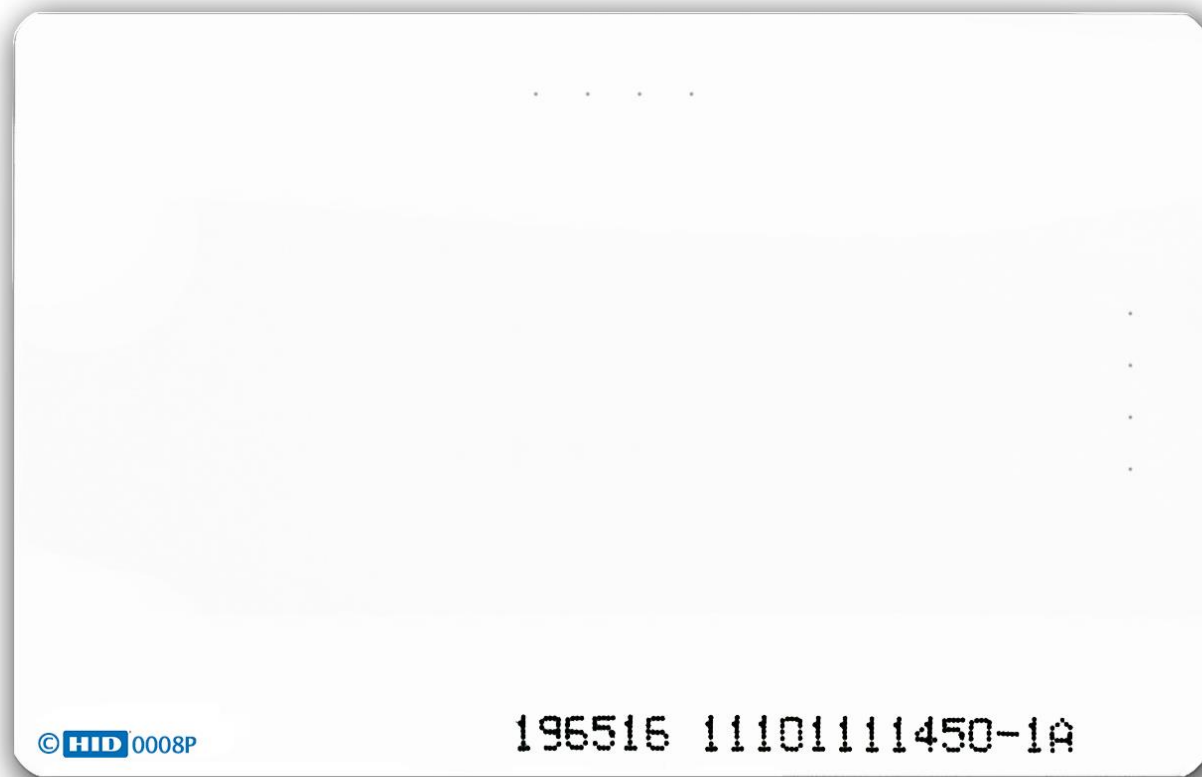


bastlíři SH

MacGyver

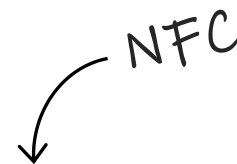
macgyver.siliconhill.cz





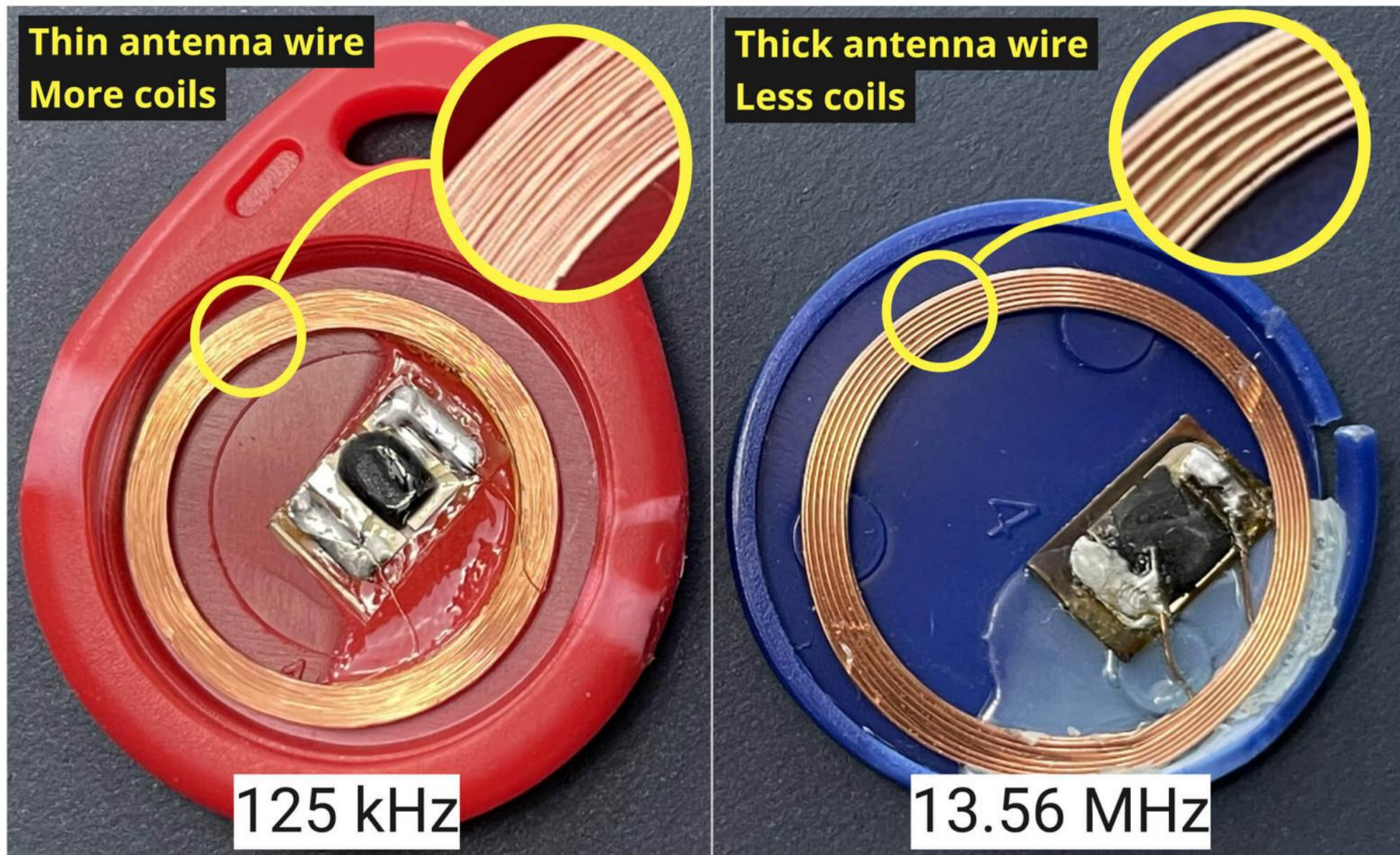
Rozdělení

Rozdělení



	LF	HF	UHF
Frekvence	125 – 134 kHz	13,56 MHz	860 – 960 MHz
Vazba	indukční	indukční	el-mag
Anténa	cívka	cívka	dipól
Vzdálenost	až 1 m	až 10 cm (ISO14443) až 1 m (ISO15693)	až 10 m
Rychlost	2 – 8 kbit/s	100 - 900 kbit/s	
Velikost	60 – 300 B	100 B – 32 kB	
Paměť (typ.)	ROM	EEPROM	EEPROM

PS: Existuje i 2.4 GHz RFID

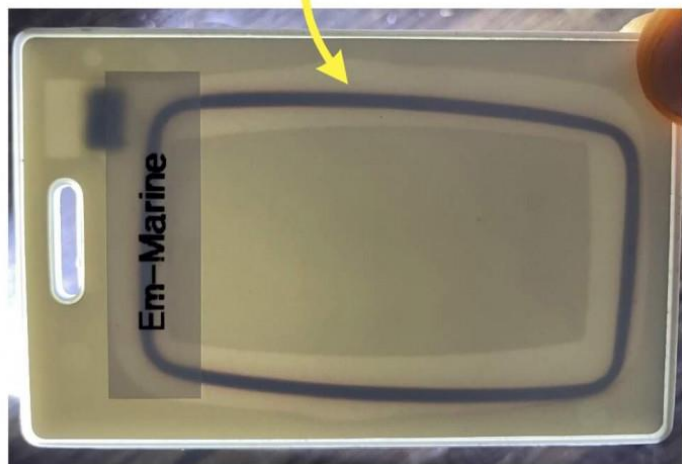


Low Frequency

125 kHz

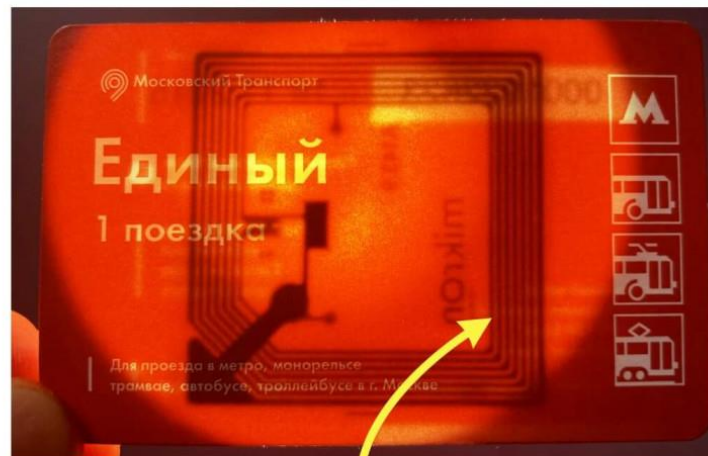


Antenna wire is thinner and has more turns
Spaces between coils are invisible

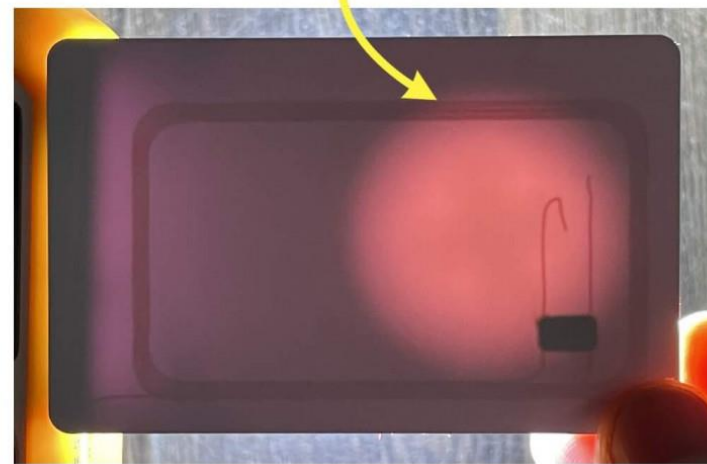


High Frequency

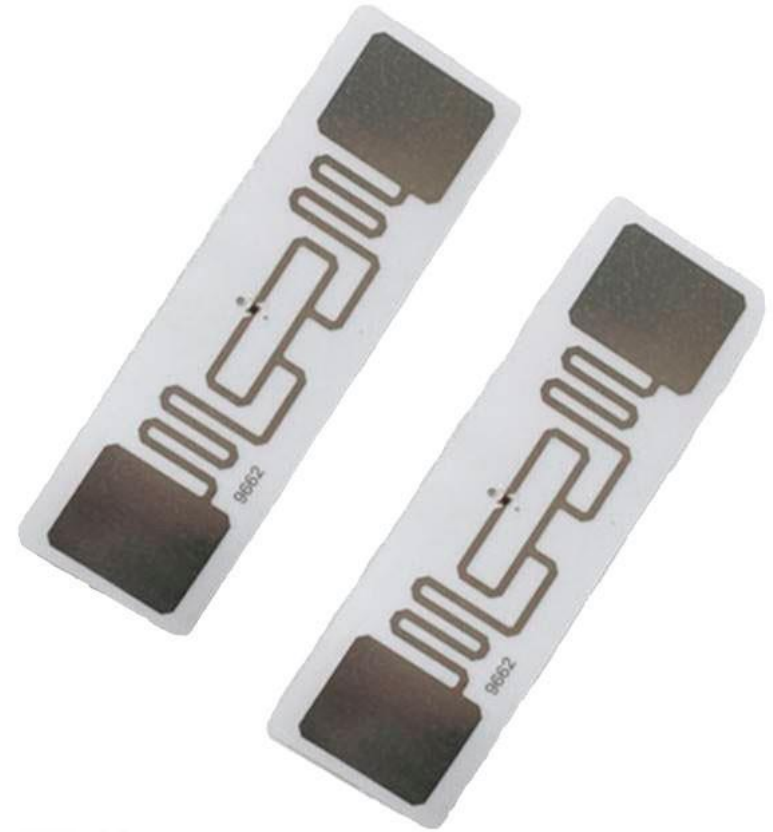
13.56 MHz



Antenna wire is wider and has less turns
Spaces between coils are recognizable

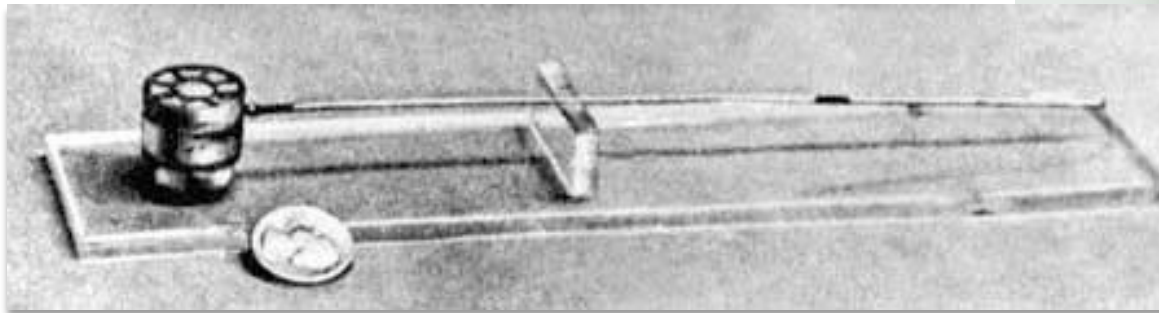


UHF

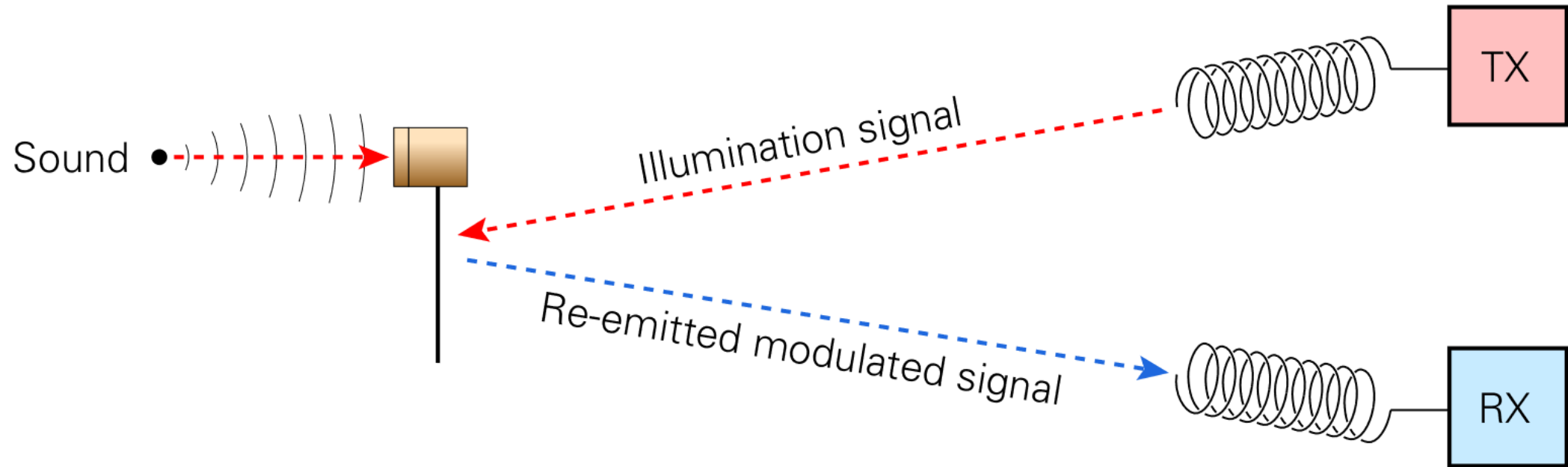


The Thing (the Great Seal bug)

- Lev Sergejevič Těrmen
- Věnováno na USA ambasádu v Moskvě (1945)
- Objeveno 1952 (7 let !)

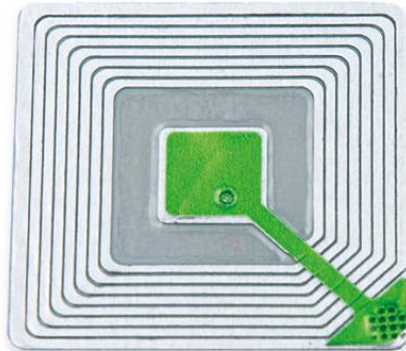


Jak to funguje?



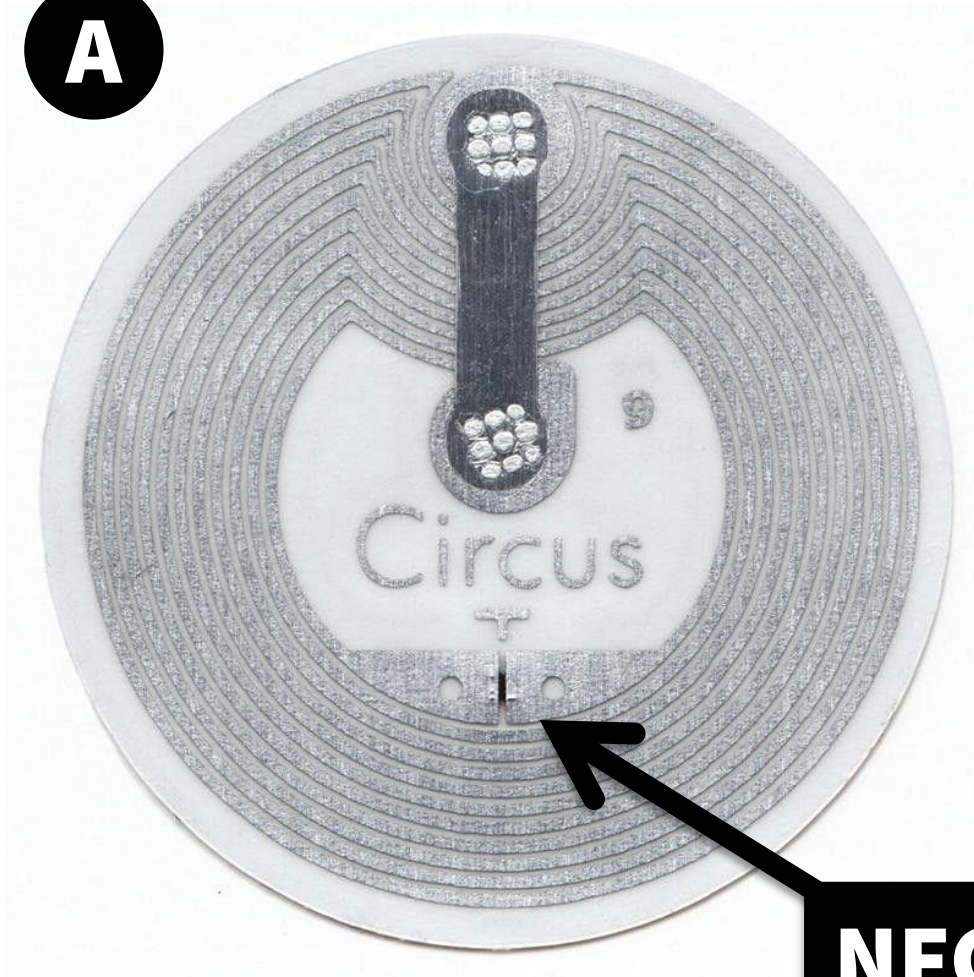
Electronic article surveillance

- Technologie:
 - Acousto-Magnetic (58 kHz)
 - Radio-Frequency (8.2 MHz)



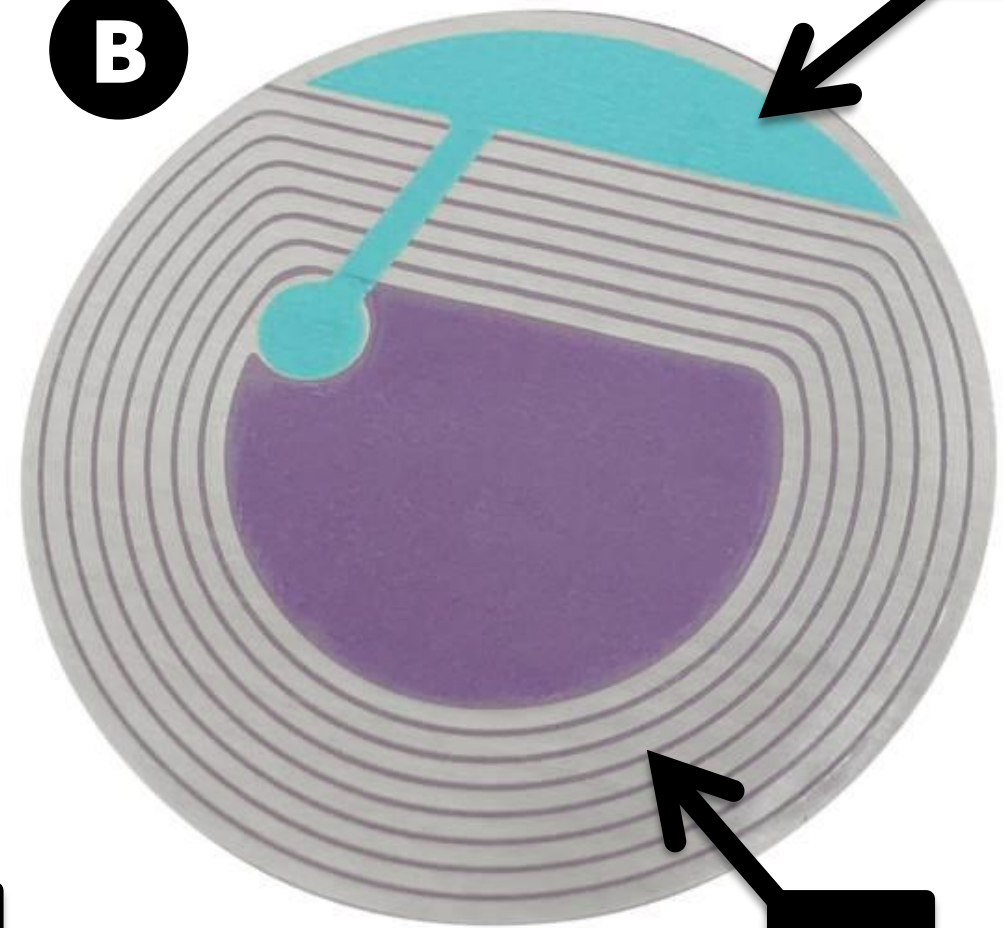
Který je NFC štítek?

A



NFC Čip

B



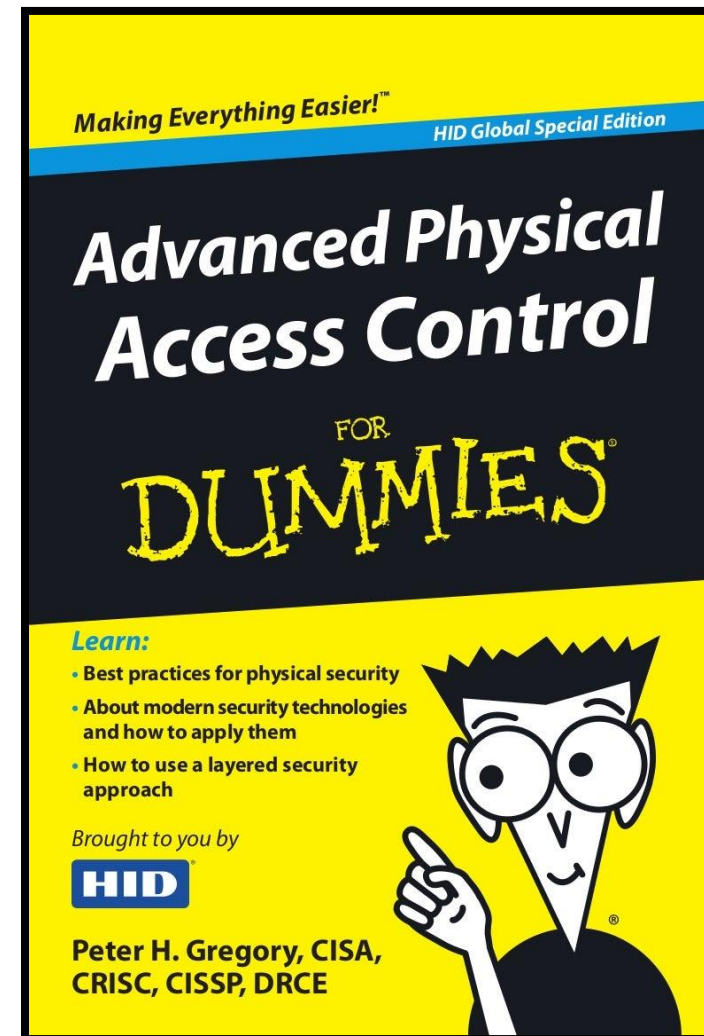
C

L

Přístupový systém

(PACS – Physical Access Control System)

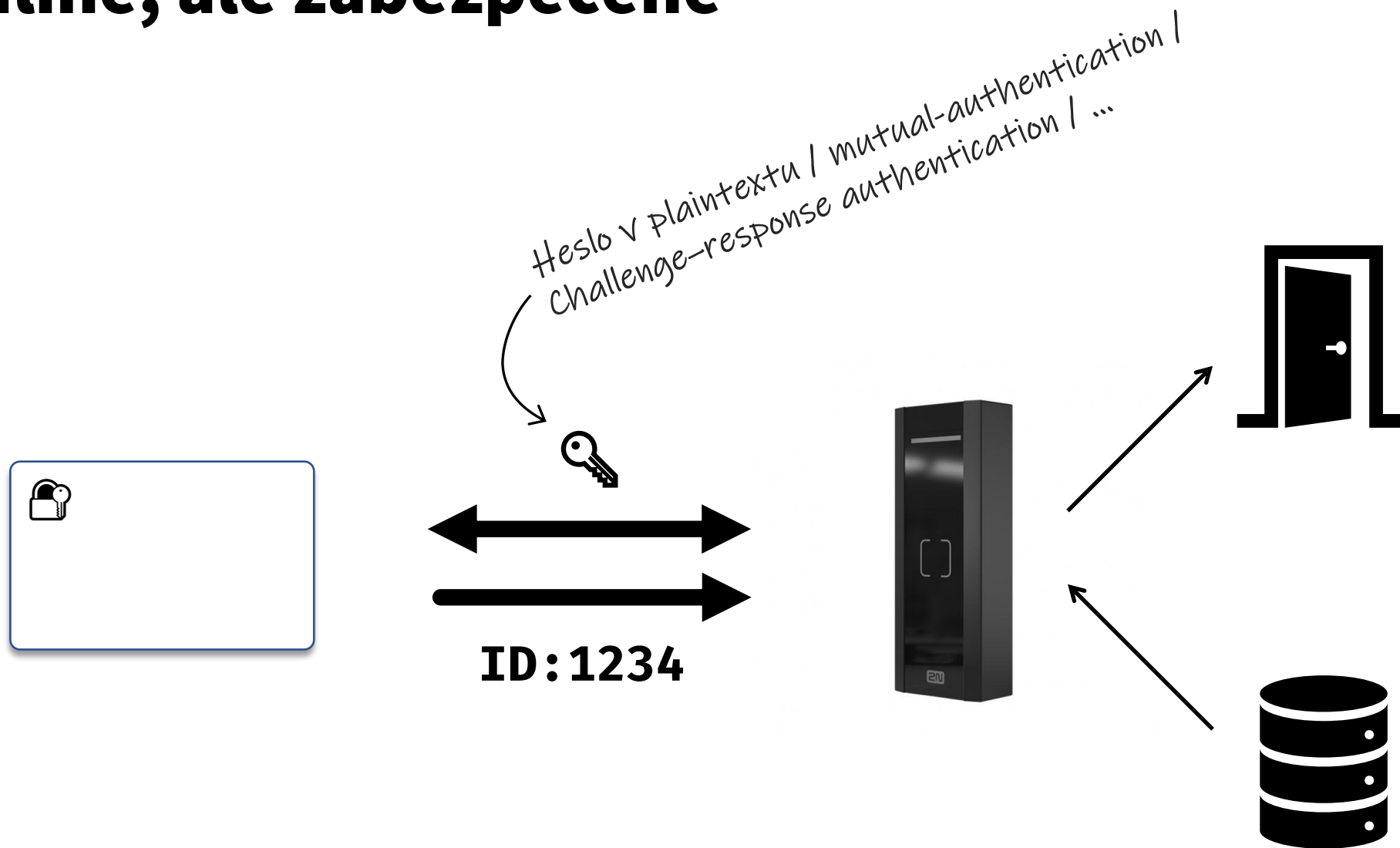
- Online
- Offline



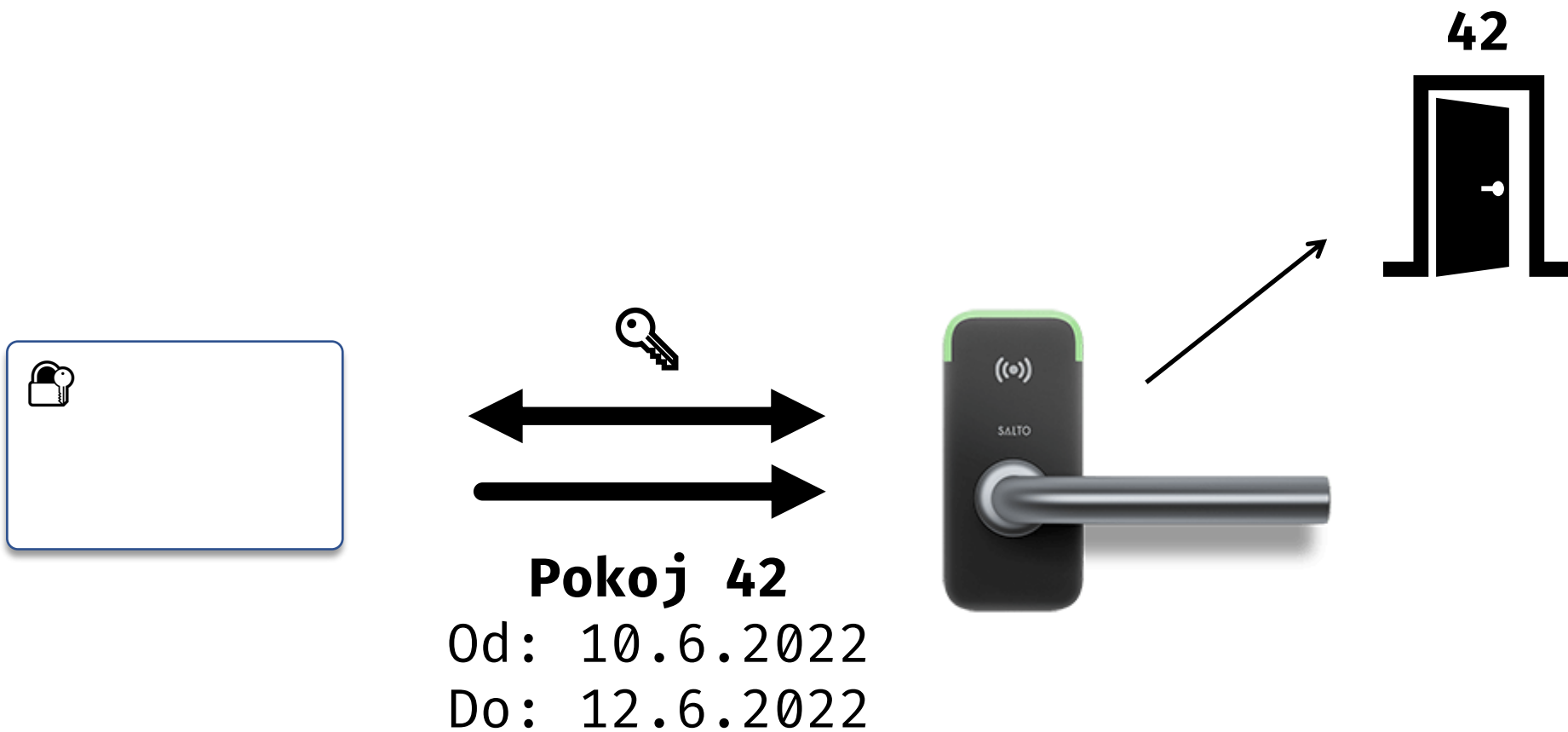
(1) Online



(2) Online, ale zabezpečeně



(3) Offline





The Big Bang Theory, S01E01

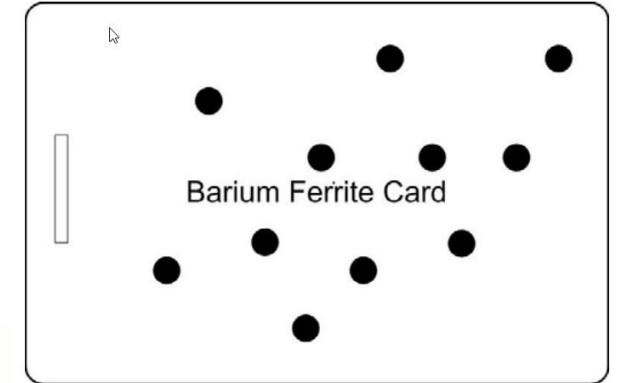
**So my neighbor put a
lock on their fence...**



LF

Co bylo před

- Magstrip
- Wiegand Card
- Barium Ferride Card





Wiegand Card





Classic Swipe Reader

Most popular Wiegand swipe reader for access control

- Rugged Wiegand swipe reader
- Power requirements: 5-12 VDC
- Dimensions: 2.3" x 5.3" x 1.7" (5.8 cm x 13.5 cm x 4.3 cm)
- Slot width: 0.062" to 0.069" (1.6 mm to 1.75 mm)
- Available in black or beige



Epic Reader

Stylish Wiegand swipe reader for access control

- Ergonomic design for easy card pass through
- Power requirements: 5-12 VDC
- Dimensions: 2.66" x 5.86" x 1.5" (6.76 cm x 14.9 cm x 3.0 cm)
- Slot width: 0.062" to 0.069" (1.6 mm to 1.75 mm)
- Available in black

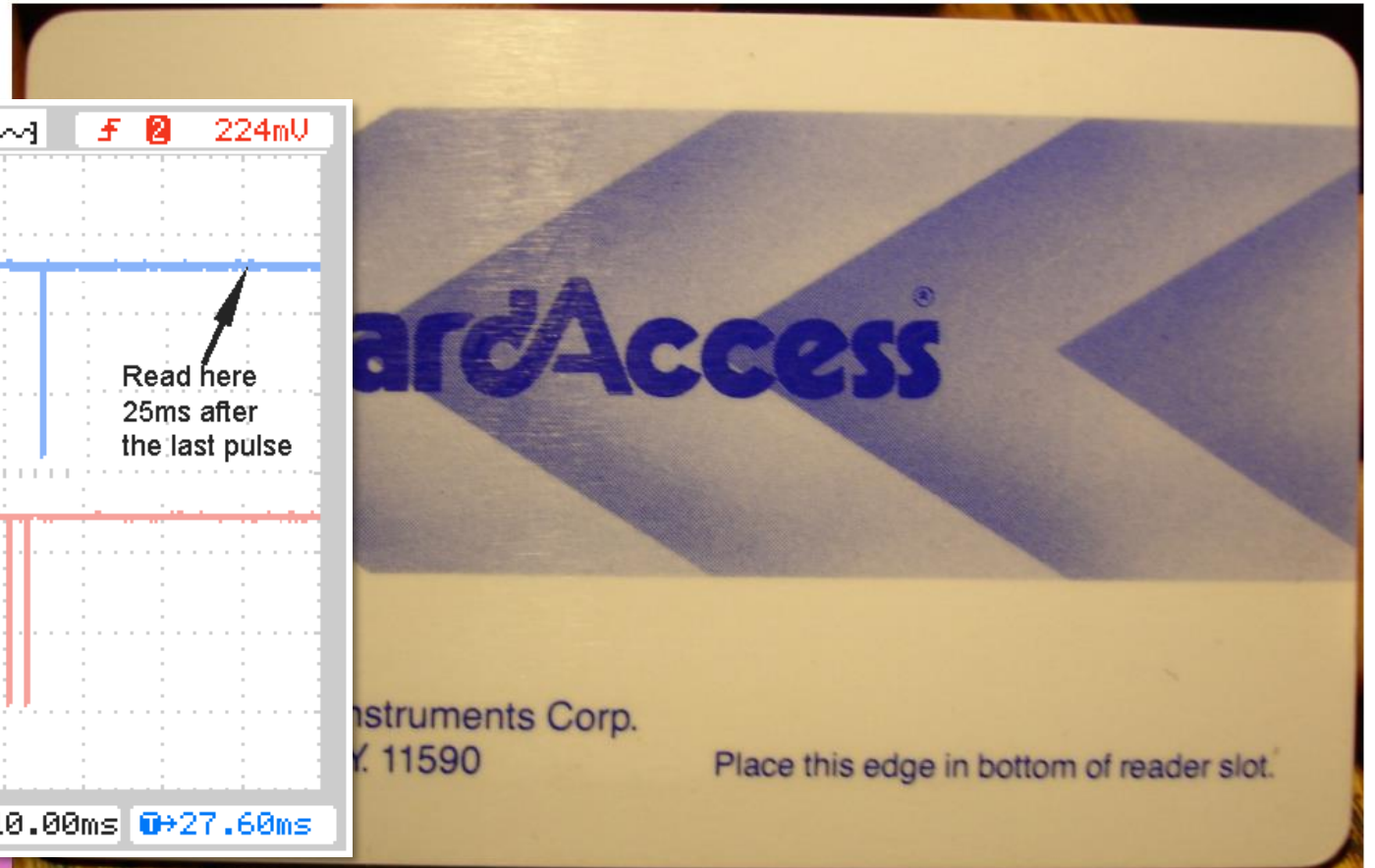
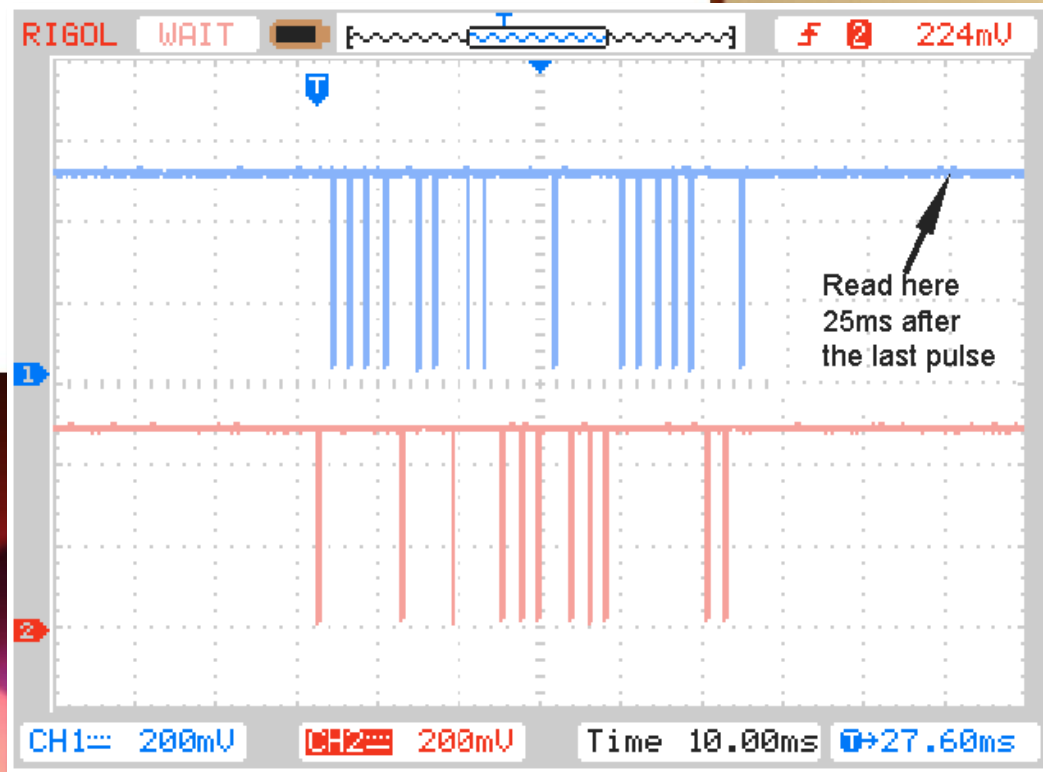


Insertion Reader

Flush mount Wiegand card reader for access control

- In-wall mounting for low profile installation
- Power requirements: 5-12 VDC
- Dimensions: 1.18" x 3.18" x 3.0" (3.0 cm x 8.1 cm x 7.6 cm)
- Slot width: 0.062" to 0.069" (1.6 mm to 1.75 mm)
- Available in chrome

Wiegand Card

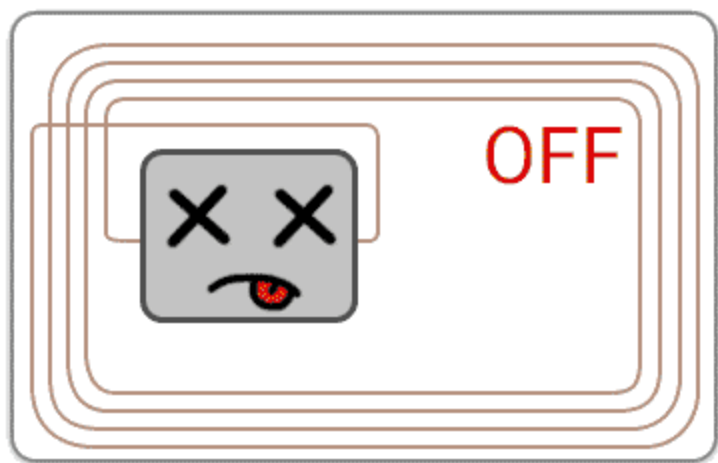


EM4100

- EM4102, EM4202, ...
- EM Microelectronic
- Cca rok 2000
- 64bit ROM
- 5 byte ID (unikátní od výroby)







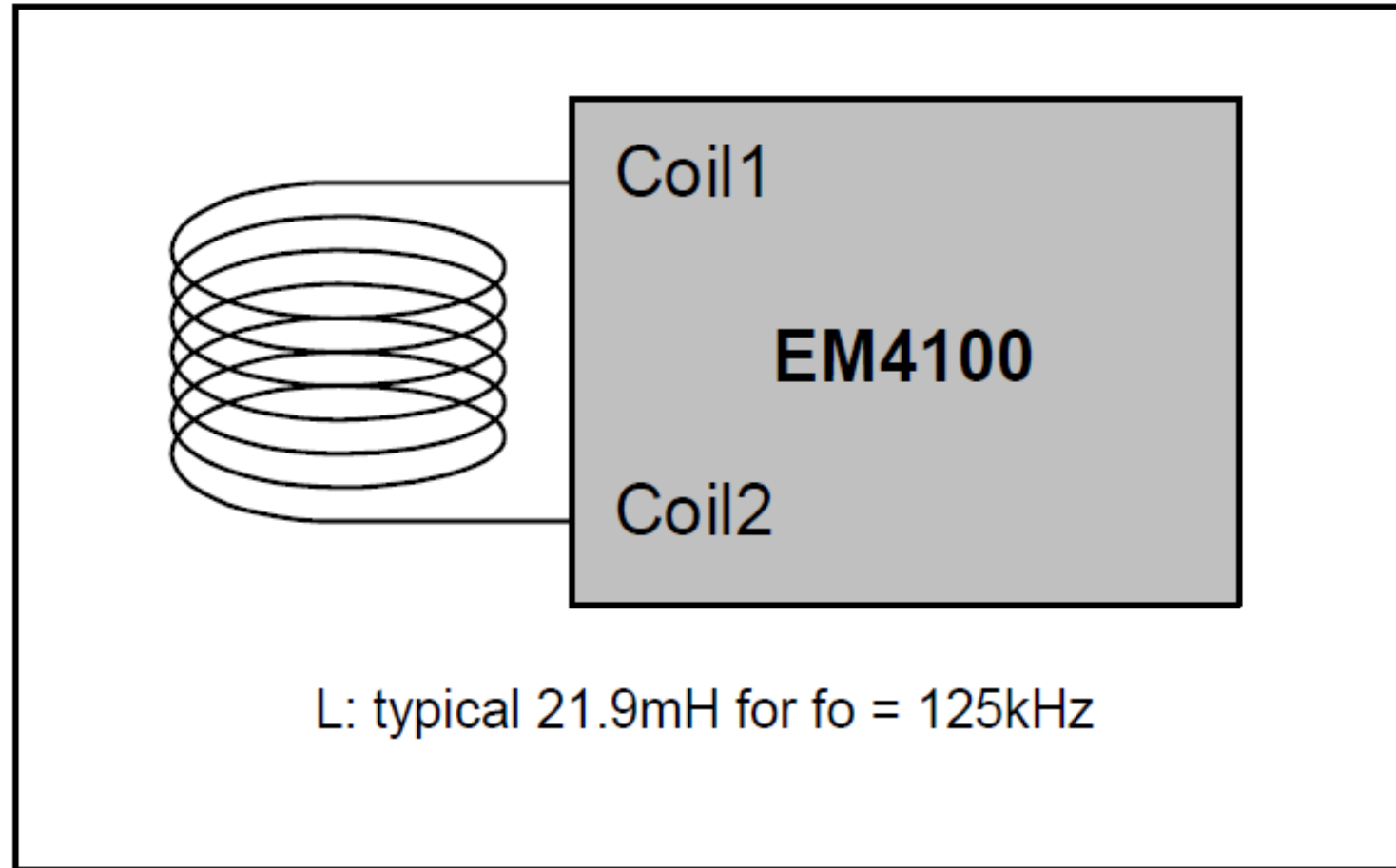


Fig. 1

System Principle

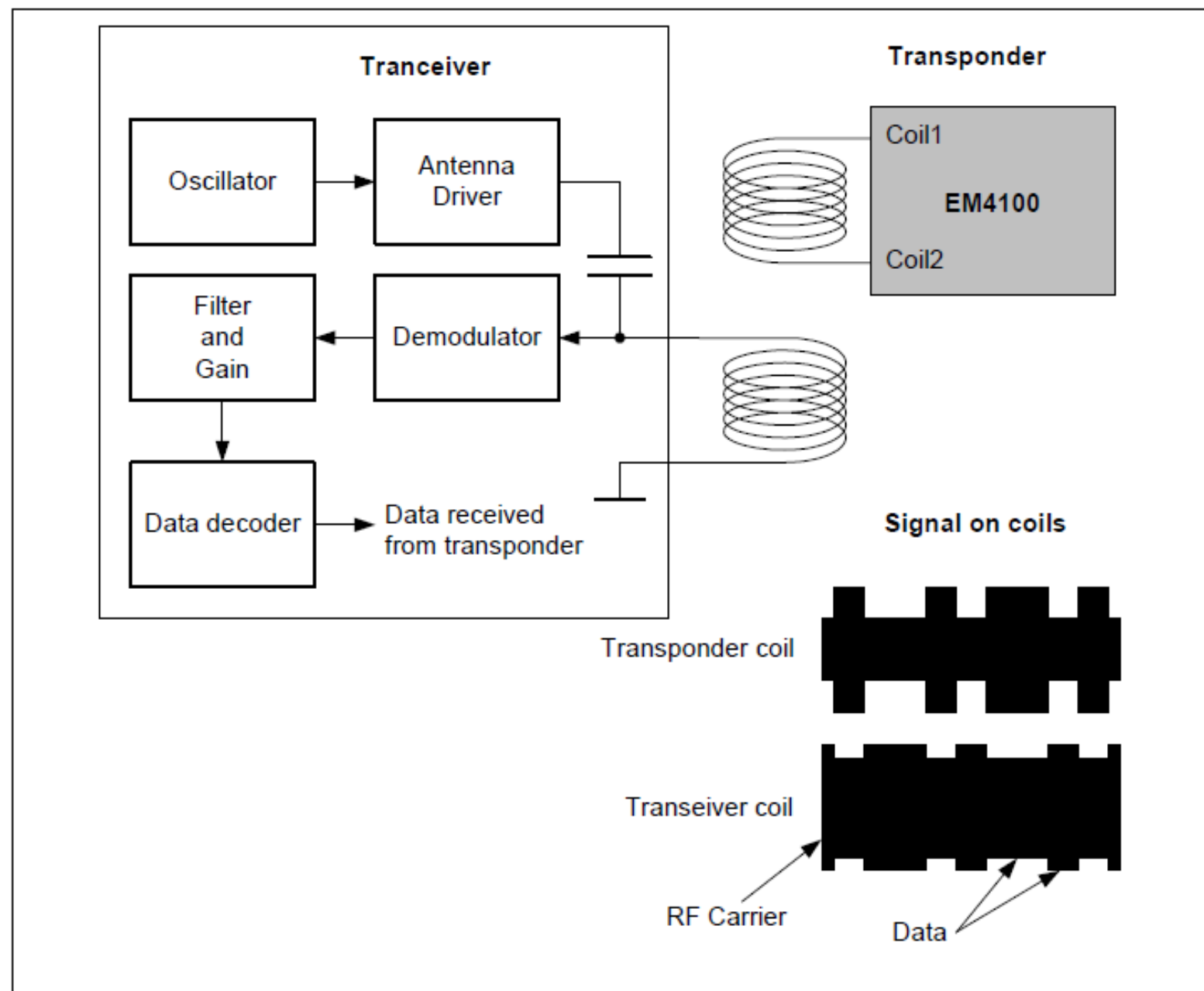


Fig. 3

Block Diagram

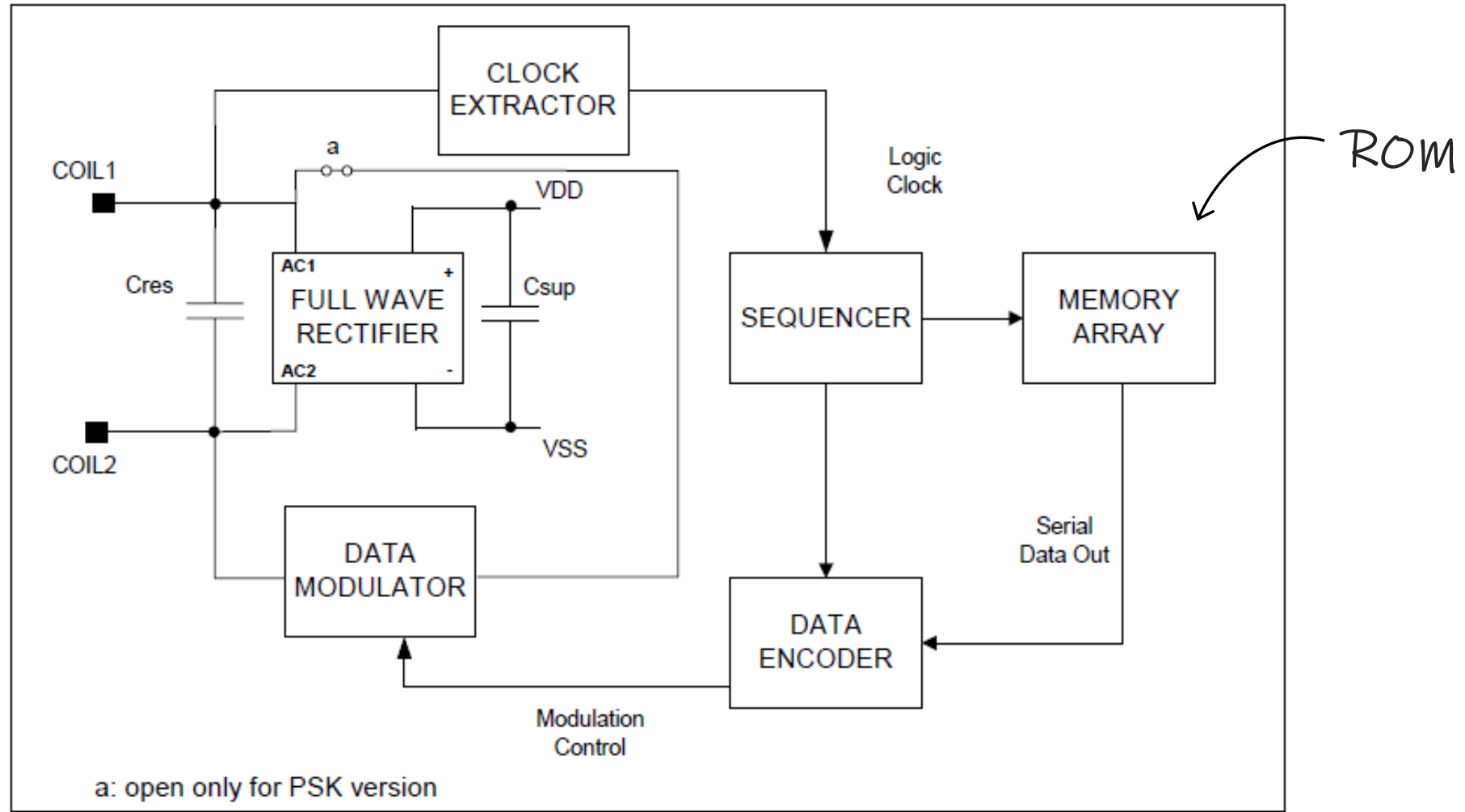
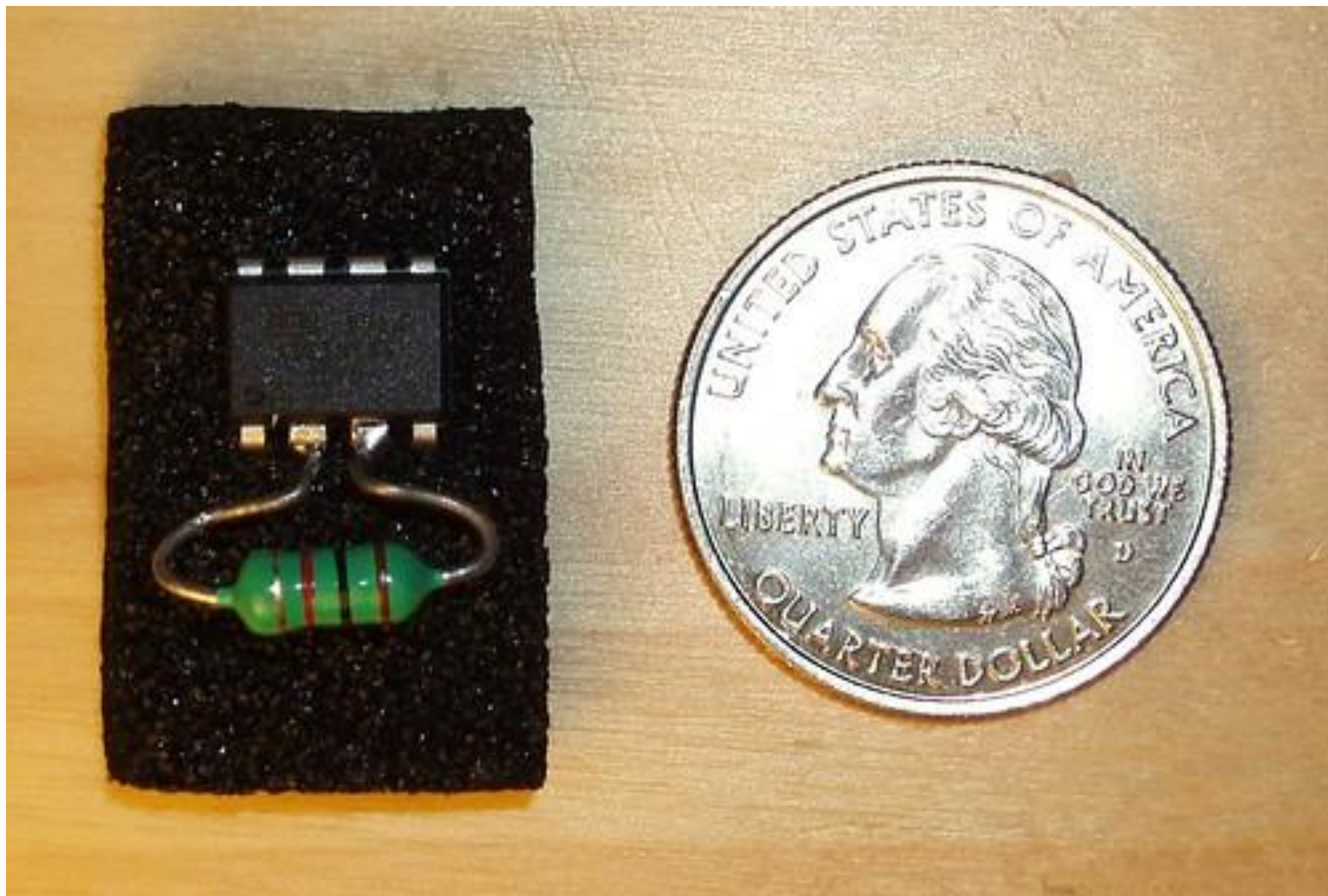


Fig. 5

1	1	1	1	1	1	1	1	1	9 header bits				
8 version bits or customer ID				D00	D01	D02	D03	P0					
				D10	D11	D12	D13	P1					
32 data bits				D20	D21	D22	D23	P2					
				D30	D31	D32	D33	P3					
				D40	D41	D42	D43	P4					
				D50	D51	D52	D53	P5					
				D60	D61	D62	D63	P6					
				D70	D71	D72	D73	P7					
				D80	D81	D82	D83	P8					
				D90	D91	D92	D93	P9					
				4 column parity bits				PC0	PC1	PC2	PC3	S0	10 line parity bits





T5577

- Obecné 125 kHz tagy
- 363bit EEPROM
- Alternativa: EM4305



ATA5577C

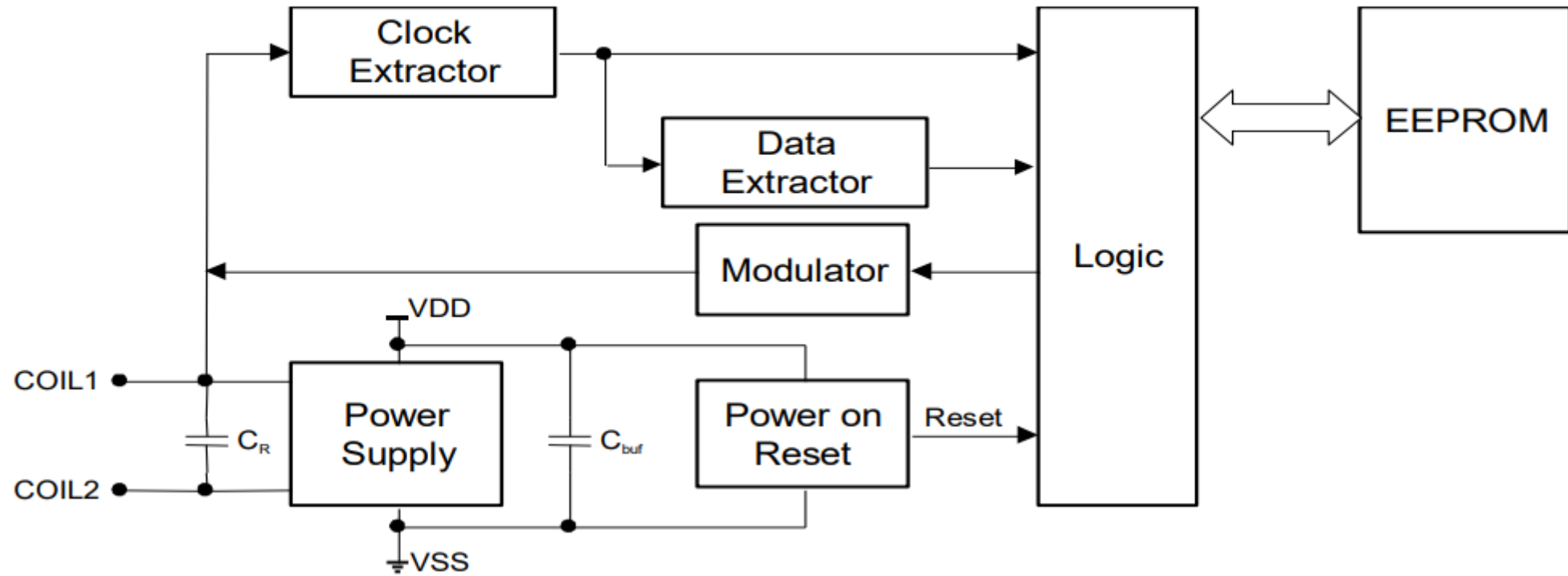
ATA5577C – Read/Write LF RFID IDIC 100 kHz to 150 kHz

Introduction

The ATA5577C is a contactless read/write Identification Integrated Chip (IDIC[®]) for applications in the 125 kHz or 134

T5577

Block Diagram



AT5577 - Příkazy

Figure 4-15. ATA5577C Command Formats Fixed Bit Length Protocol and Long Leading Reference Protocol

	Ref	OP
Standard write	R**)	1p*) L 1 Data 32 2 Addr 0
Protected write	R**)	1p*) 1 Password 32 L 1 Data 32 2 Addr 0
AOR (wake-up command)	R**)	1p*) 1 Password 32
Direct access (PWD = 1)	R**)	1p*) 1 Password 32 0 2 Addr 0
Direct access (PWD = 0)	R**)	1p*) 0 2 Addr 0
Page 0/1 regular read	R**)	1p*)
Reset command	R**)	00

*) p = page selector
 **) R = R0, R1, R2, R3, R4, R5, R6, R7, R8, R9, R10, R11, R12, R13, R14, R15

^{*}) p = page selector

***) R = Reference pulse if necessary

T5577 – EEPROM

Figure 3-2. Memory Map

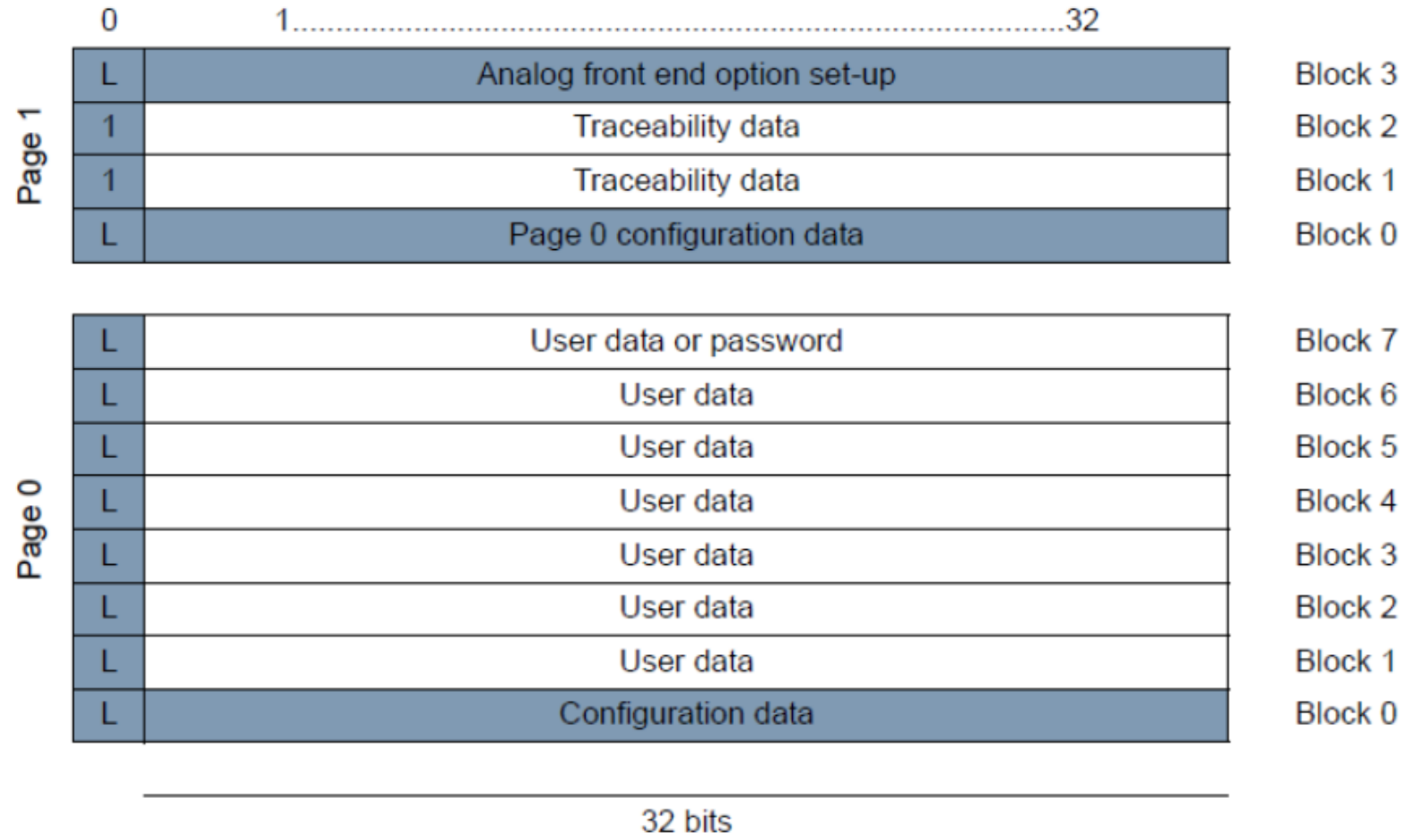


Table 5-2. Block 0 Page 0 – Configuration Mapping in Basic Mode

L	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32			
					0	0	0	0	0	0	0				0								0						0	0					
Lock Bit	Master Key (1), (2)												Data Bit Rate				Modulation								PSKCF		AOR		MAX BLOCK		PWD	ST Sequence Terminator			Init Delay
	0 Unlocked												RF/8 0 0 0								0 0		RF/2												
																											1 Locked								
													RF/32 0 1 0								1 0		RF/8												
													RF/50 1 0 0				0	0	0	0	0	Direct													
																													RF/64 1 0 1				0	0	0
													RF/100 1 1 0																				0	0	0
																													RF/128 1 1 1				0	0	0
																																	0	0	1
																																	0	0	1
																																	0	0	1
																																	0	0	1
																0																	1	0	0
																																1	0	0	0
																																1	1	0	0

- Notes:
1. If the *Master Key* is 6 the test mode access is disabled
 2. If the *Master Key* is neither 6 nor 9, the extended function mode and *Init Delay* are disabled

[usb] pm3 → lf t55xx clonehelp

For cloning specific techs on T55xx tags, see commands available in corresponding LF sub-menus,

lf awid clone

lf destron clone

lf em 410x clone

lf fdxb clone

lf gallagher clone

lf gproxii clone

lf hid clone

lf indala clone

lf io clone

lf jablotron clone

lf kerl clone

lf motorola clone

lf nedap clone

lf nexwatch clone

lf noralsy clone

lf pac clone

lf paradox clone

lf presco clone

lf pyramid clone

lf securakey clone

lf viking clone

lf visa2000 clone



HF

HF

- ISO 14443A/B (Proximity)
- ISO 15693 (Vicinity)
- ISO 18092 (NFC)
- JIS: X6319-4 (Felica)
- NFC Forum Technical Specifications
- ...

ISO14443

- 14443-1 Part 1: Physical characteristics

- 14443-2 Part 2: Radio frequency power and signal interface

- 14443-3 Part 3: Initialization and anticollision

- 14443-4 Part 4: Transmission protocol

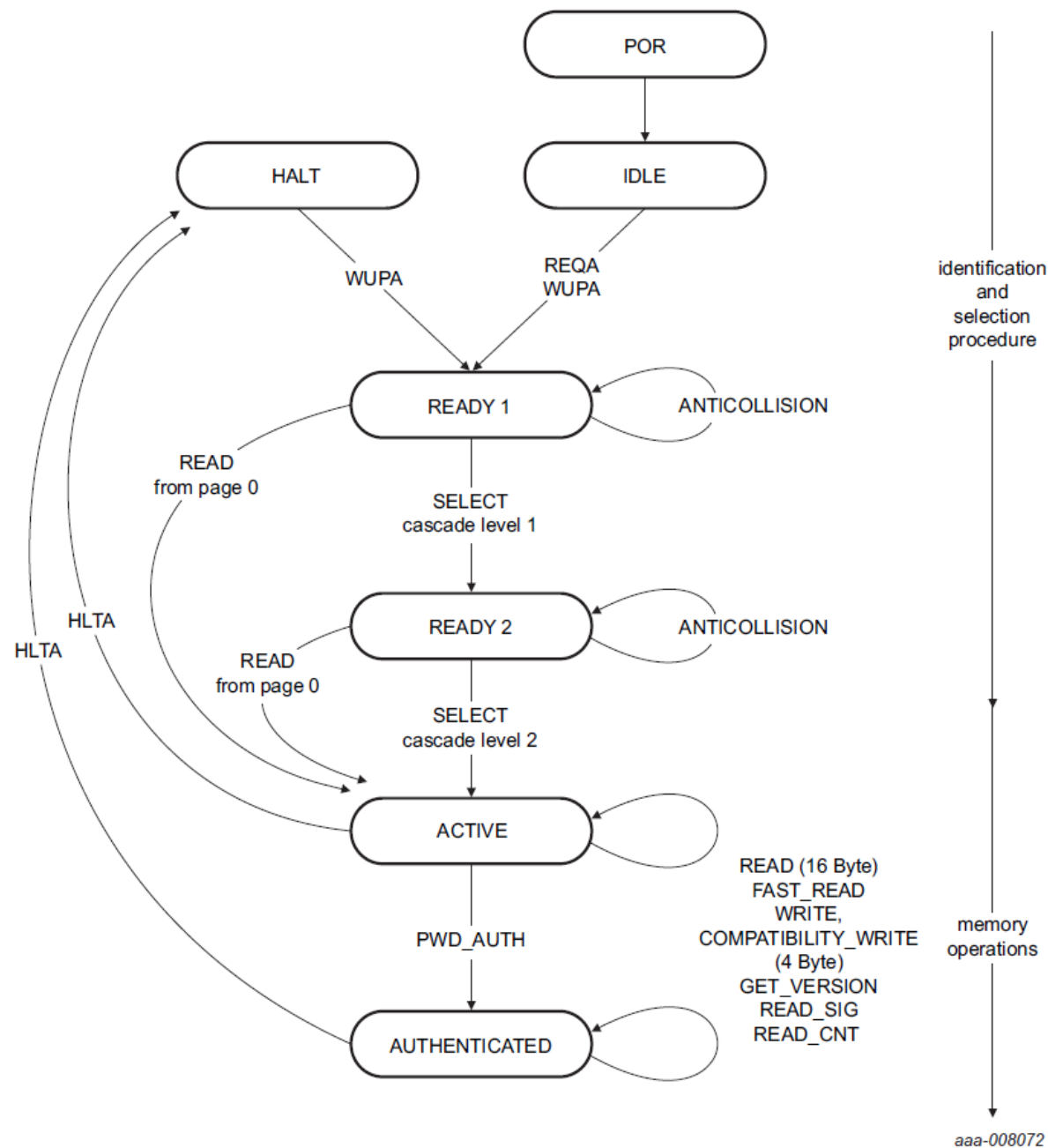
RF Modulace, Rychlost

Antikolizní mechanismus,
přenos UID, select

ISO7816

NTAG 213

(ISO14443A-3)



Remark: In all states, the command interpreter returns to the idle state on receipt of an unexpected command. If the IC was previously in the HALT state, it returns to that state.

NTAG 213

(ISO14443A-3)

Table 22. Command overview

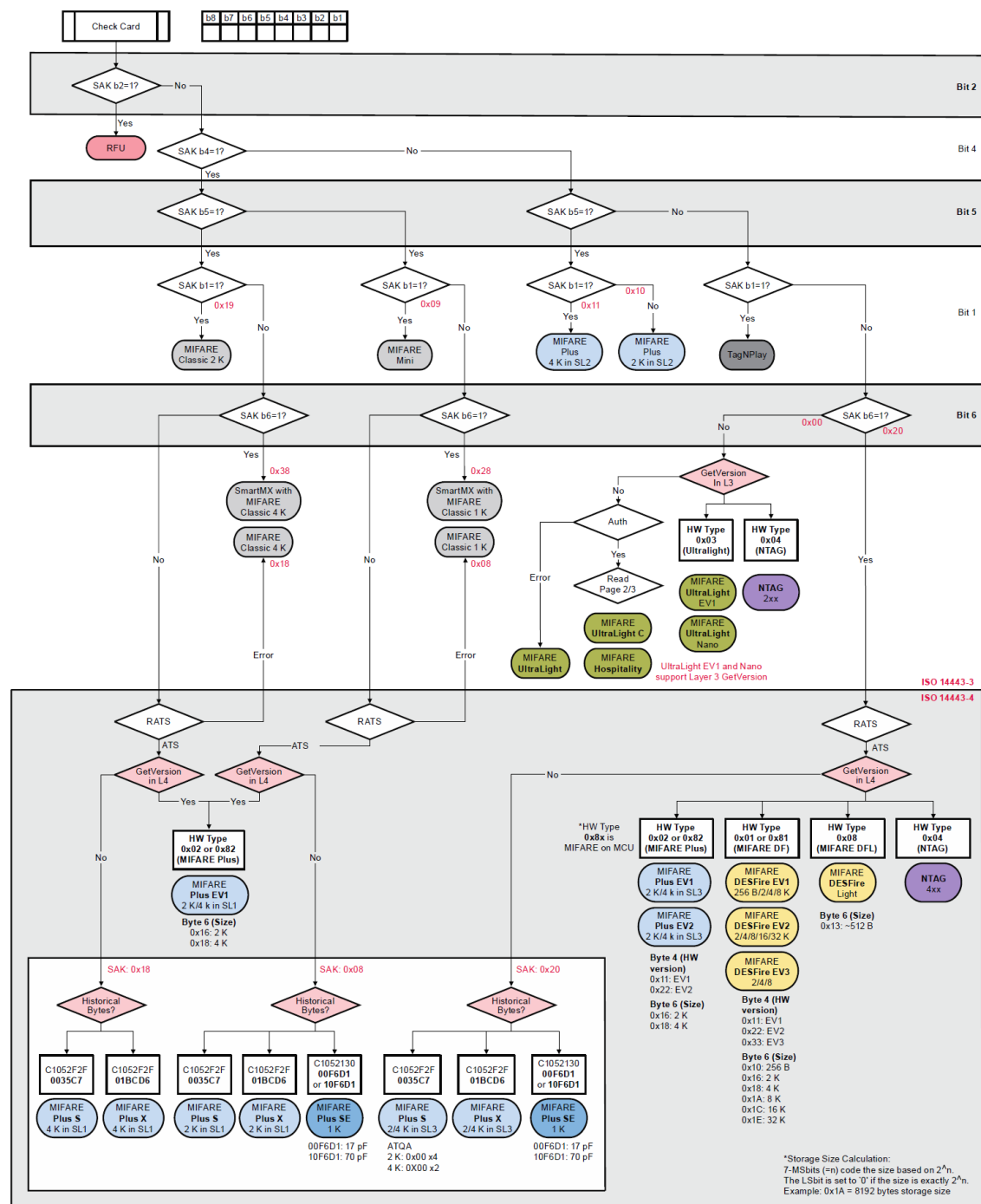
Command ^[1]	ISO/IEC 14443	NFC FORUM	Command code (hexadecimal)
Request	REQA	SENS_REQ	26h (7 bit)
Wake-up	WUPA	ALL_REQ	52h (7 bit)
Anticollision CL1	Anticollision CL1	SDD_REQ CL1	93h 20h
Select CL1	Select CL1	SEL_REQ CL1	93h 70h
Anticollision CL2	Anticollision CL2	SDD_REQ CL2	95h 20h
Select CL2	Select CL2	SEL_REQ CL2	95h 70h
Halt	HLTA	SLP_REQ	50h 00h
GET_VERSION ^[2]	-	-	60h
READ	-	READ	30h
FAST_READ ^[2]	-	-	3Ah
WRITE	-	WRITE	A2h
COMP_WRITE	-	-	A0h
READ_CNT ^[2]	-	-	39h
PWD_AUTH ^[2]	-	-	1Bh
READ_SIG ^[2]	-	-	3Ch

[1] Unless otherwise specified, all commands use the coding and framing as described in [Ref. 1](#).

[2] This command is new in NTAG21x compared to NTAG203.

AN10833

MIFARE type identification procedure



ISO14443A-3

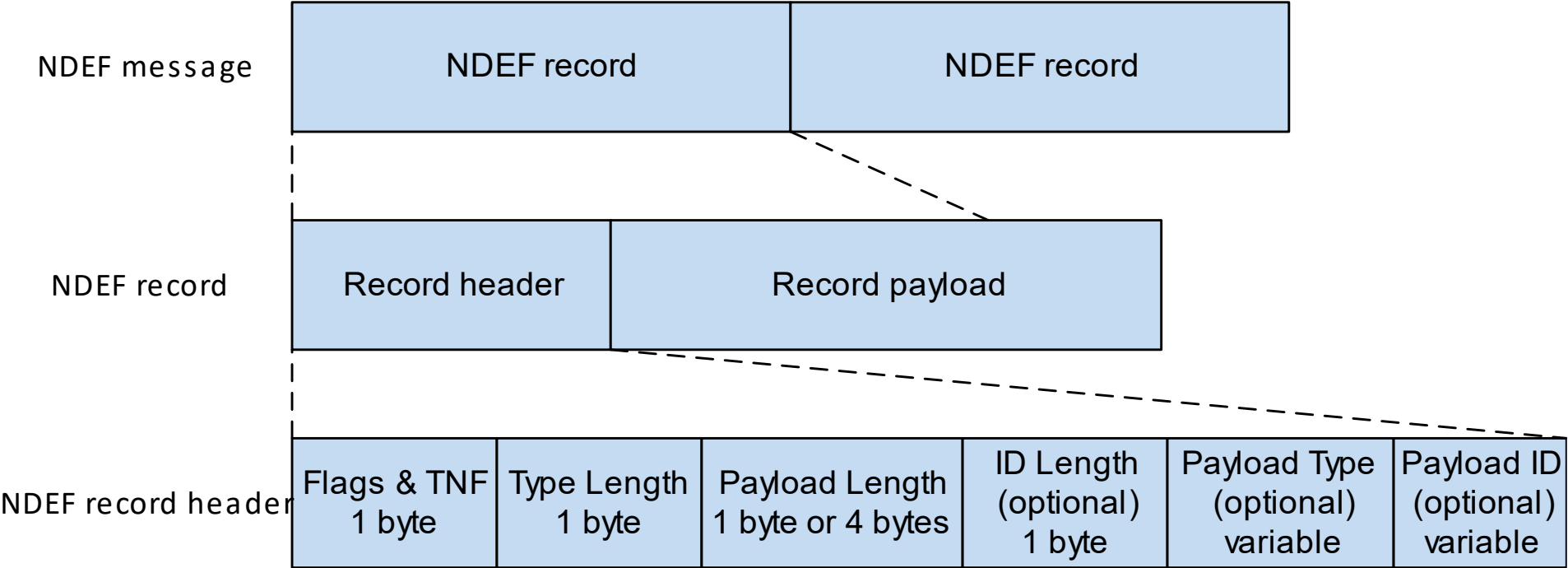
ISO14443A-4

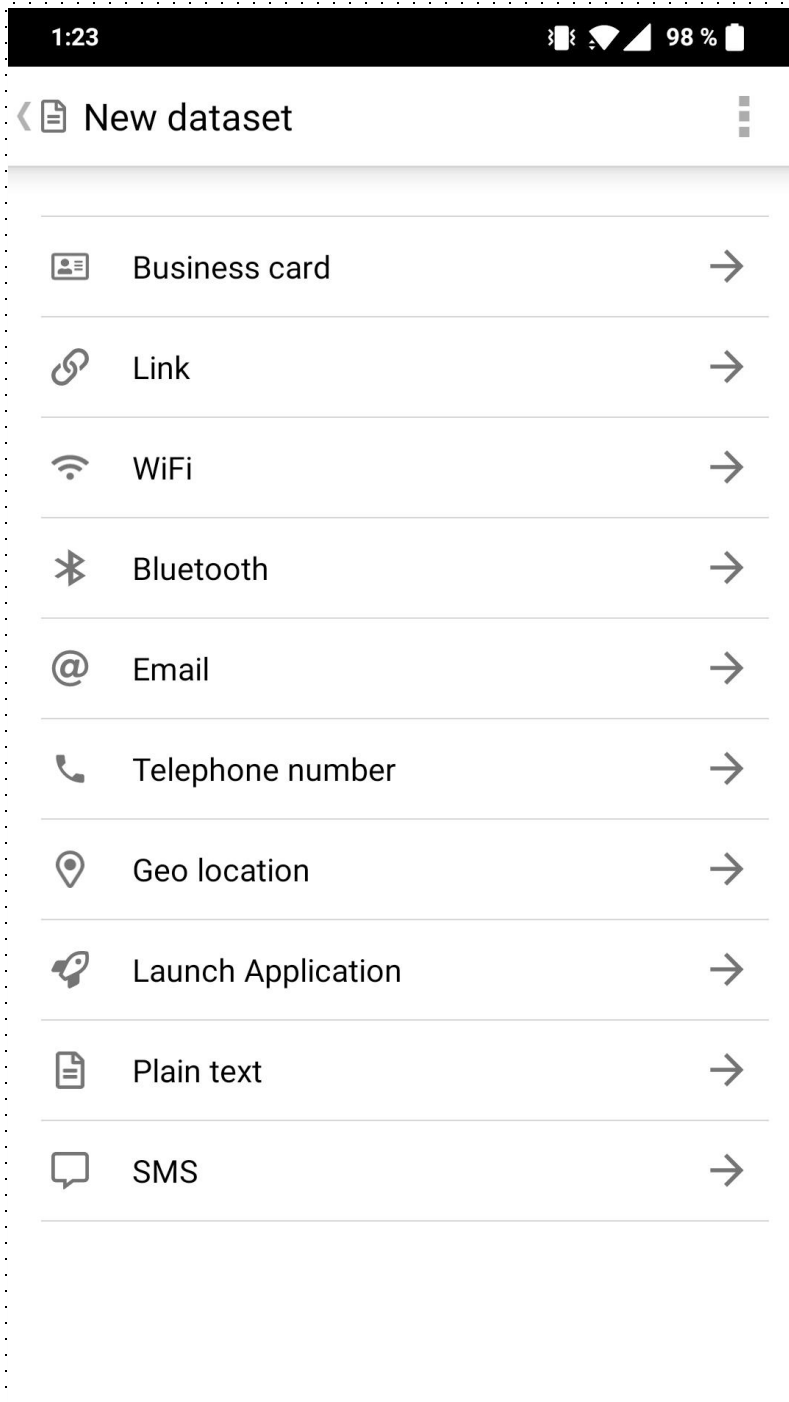
NFC Tag

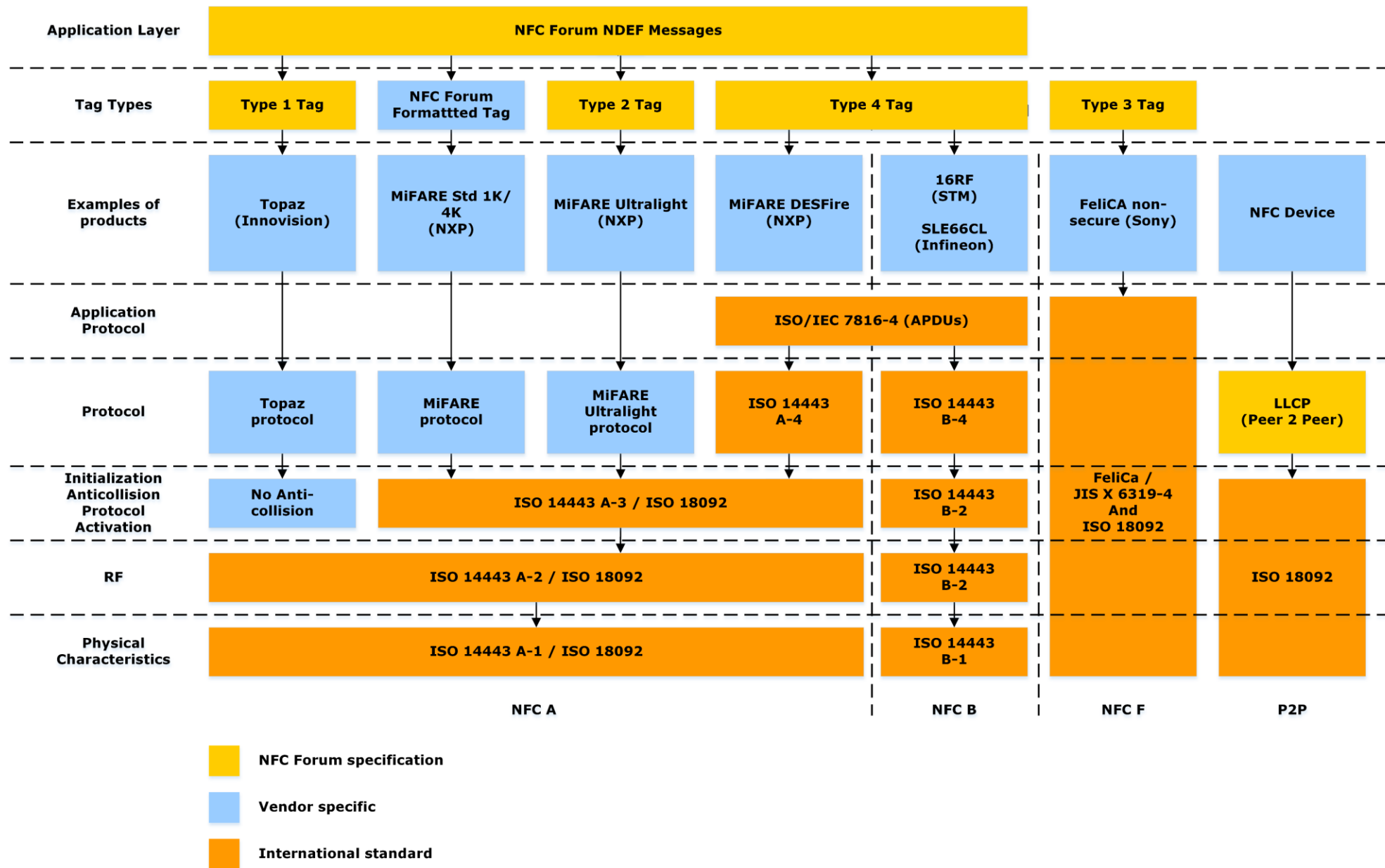
NFC Tag

- NFC Forum (<https://nfc-forum.org/>)
- NDEF Message
- Unifikovaný způsob jak číst data

NDEF



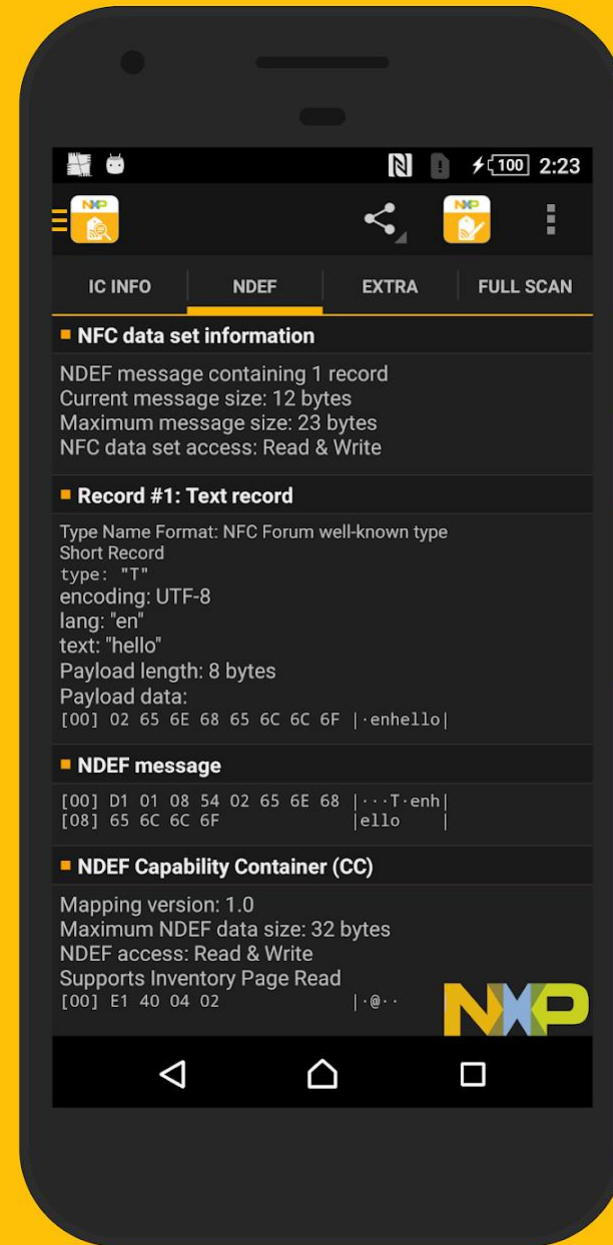




Nástroje

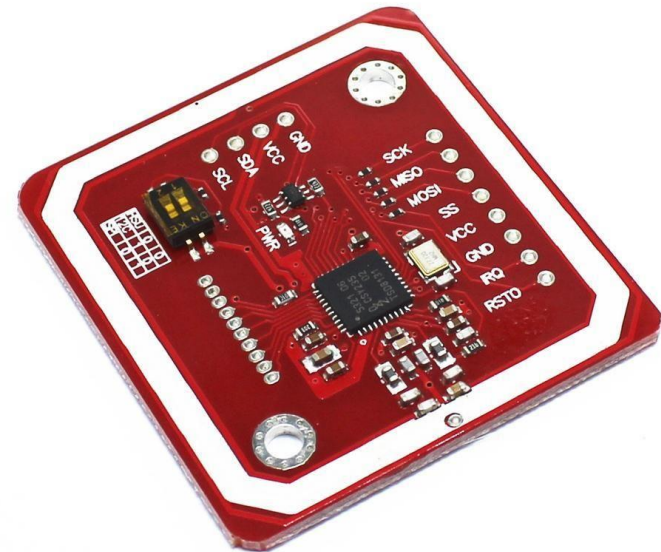
Pro Android

- NXP TagInfo
- NXP TagWriter
- MetroDroid
- NFC tools, ...



DYI

- RC522 + Arduino
- PN532 + USB 2 UART + Lib-nfc



Proxmark

- „SDR“
- švýcarský nůž pro RFID
- Vývoj od 2007
- Ohromná komunita



- <https://lab401.com/products/proxmark-3-rdv4>
- <https://github.com/Proxmark/proxmark3>
- <https://github.com/RfidResearchGroup/proxmark3>

Flipper Zero

- Kickstarter 2020
- RF (CC1101), BLE, RFID, NFC, IR, iButton, ...



Kam dál

- <https://blog.flipperzero.one/rfid/>
- <https://github.com/doegox/awesome-rfid-talks>
- Proxmark Discord a Forum
- <https://github.com/RfidResearchGroup/proxmark3>

Zajímavosti

FIDO

- Např. YubiKey 5 NFC
 - ISO14443-4 (ISO7816)
 - NFC aplikační vrstva je přímo ve FIDO sepc.
-
- YubiKey navíc může obsahovat NFC Tag Type-4 NDEF zprávu
 - **OATH-HOTP** (<https://www.yubico.com/resources/glossary/oath-hotp/>) nebo
 - **Yubico OTP** (<https://developers.yubico.com/OTP/>)
 - nebo statické heslo
 - V podobě URL (uživatelky definované) nebo TXT



Apple AirTag

- nRF52832
- NFC-A peripheral
 - Implementují NFC Tag Type-4
 - Pouze ke čtení
- Obsahuje NDEF Msg s URL např.:

```
https://found.apple.com/airtag?pid=5500&b=00&pt=004c&fv=0010  
0e10&dg=00&z=00&bt=A0B1C2D3E4F5&sr=ABCDEF123456&bp=0015
```



Platební karta

- EMV (Europay, Mastercard, and Visa)
- ISO7816 (kontaktní) a ISO 14443 (bezkontaktní)

Biometrický pas



- ISO 14443-4
- Patří mezi MRTD (Machine Readable Travel Documents)
 - Definuje ICAO (International Civil Aviation Organization)
 - Dokument **9303** (má 13 částí)
<https://www.icao.int/publications/pages/publication.aspx?docnum=9303>
- Zabezpečení
 - RID
 - Datové soubory jsou podepsané (PKI)
 - BAC (Basic Access Control) – challenge-response, terminál musí znát MRZ
 - AA (Active Auth.) – pas má vlastní priv. klíč a může vám něco podepsat

Tiskárna DYMO 500

- Termo tiskárna štítků
- Tiskne jen na štítky s RFID tagem (originální od výrobce, DRM)
- NXP icode SLIX2 (ISO 15693)
- 16 bit counter
 - Začíná na 0xFFFF – počet štítků
 - Při tisku se inkrementuje (read password může jen inkrementovat)
 - 0xFFFF je prázdná špulka



Otázky?

@horcicaa

adam@horcica.cz

MacGyver
macgyver.siliconhill.cz