

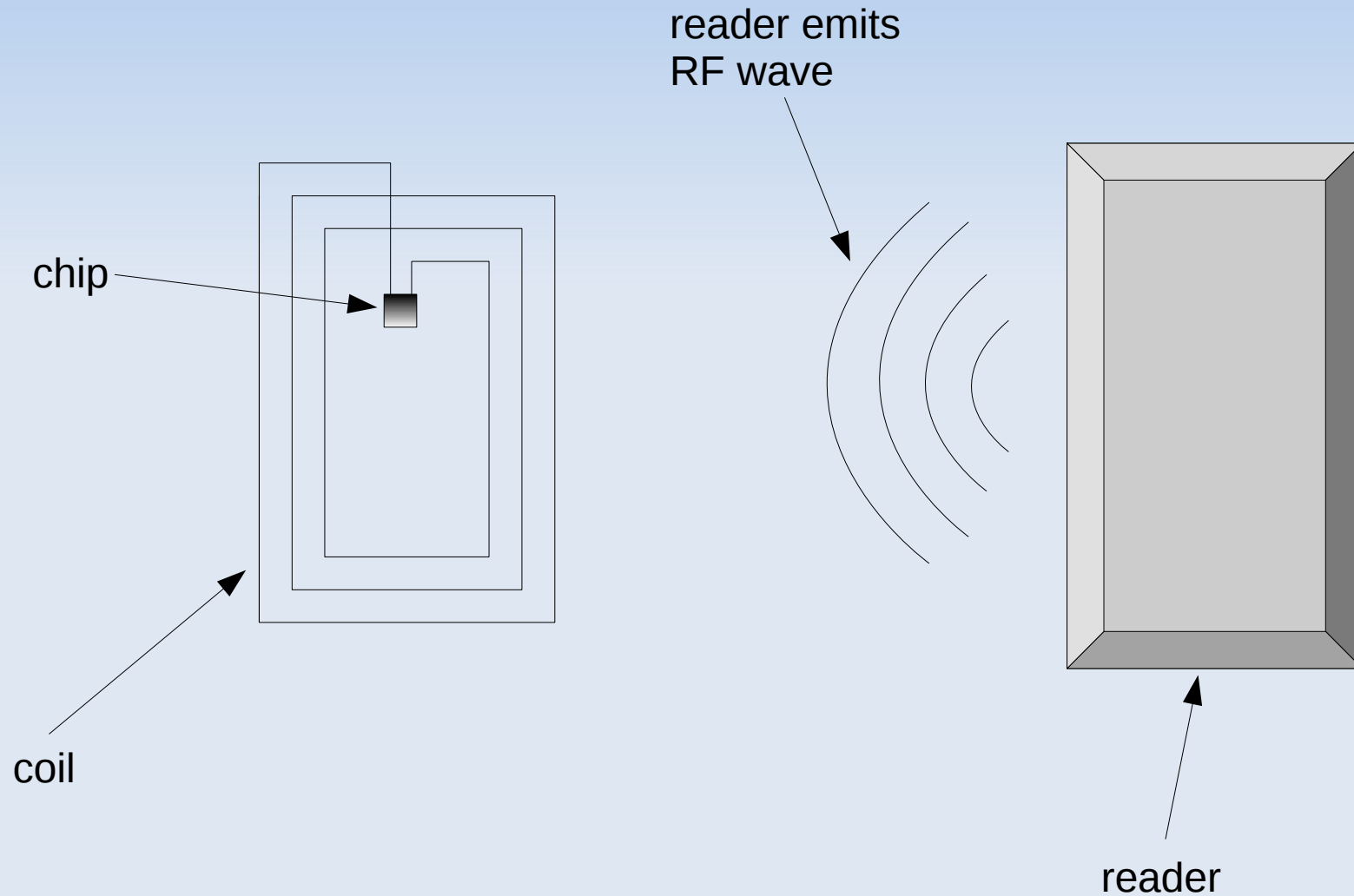
# Introduction to RFID/NFC

- Alan Carvalho de Assis

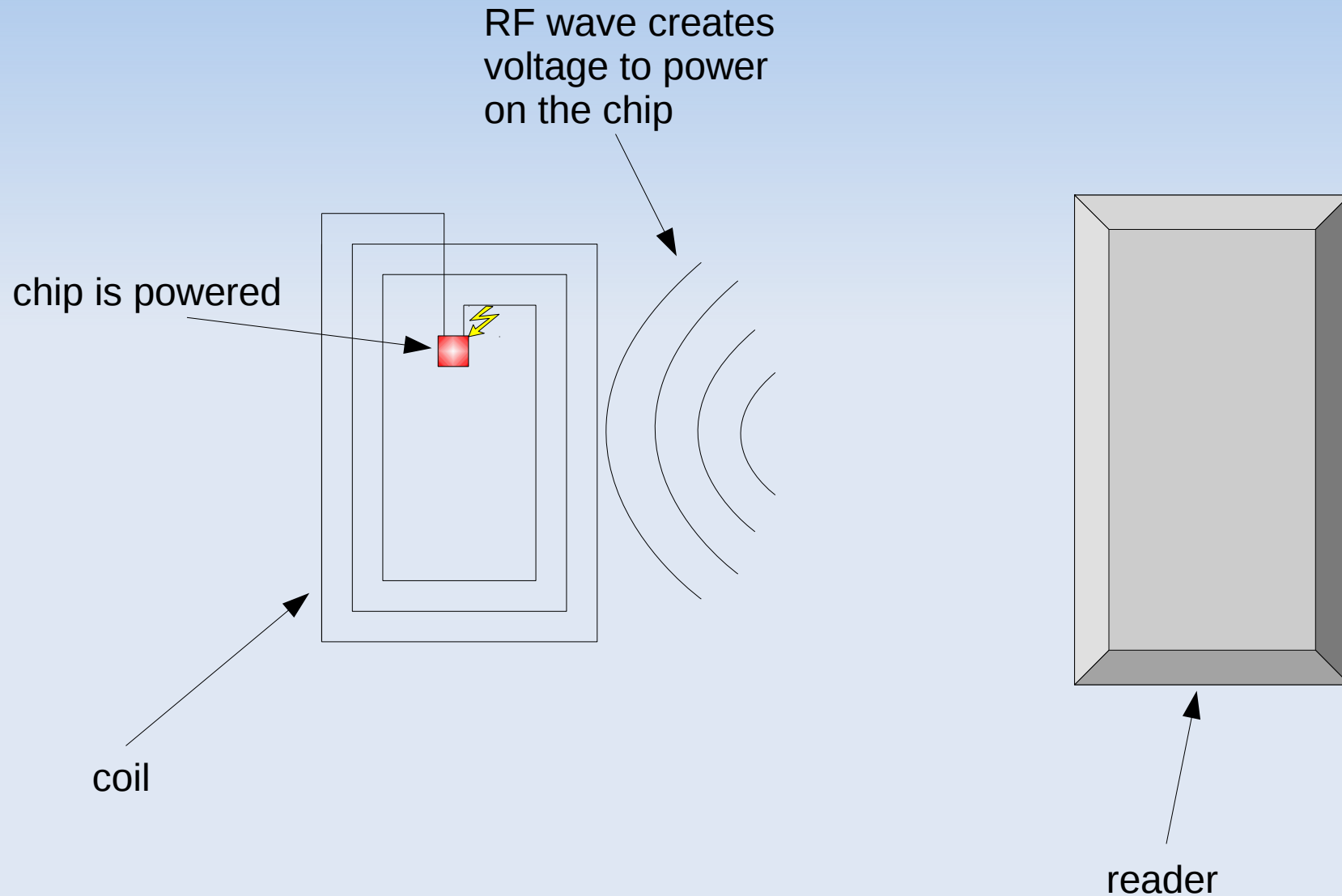
# What is RFID?

- RFID = Radio-Frequency Identification
- RFID Device = TAG or Transponder;
- Simple RFID:
  - Only TAG to Reader communication;
- Powerful RFID:
  - Bi-directional communication;
  - AKA: contactless smartcard.

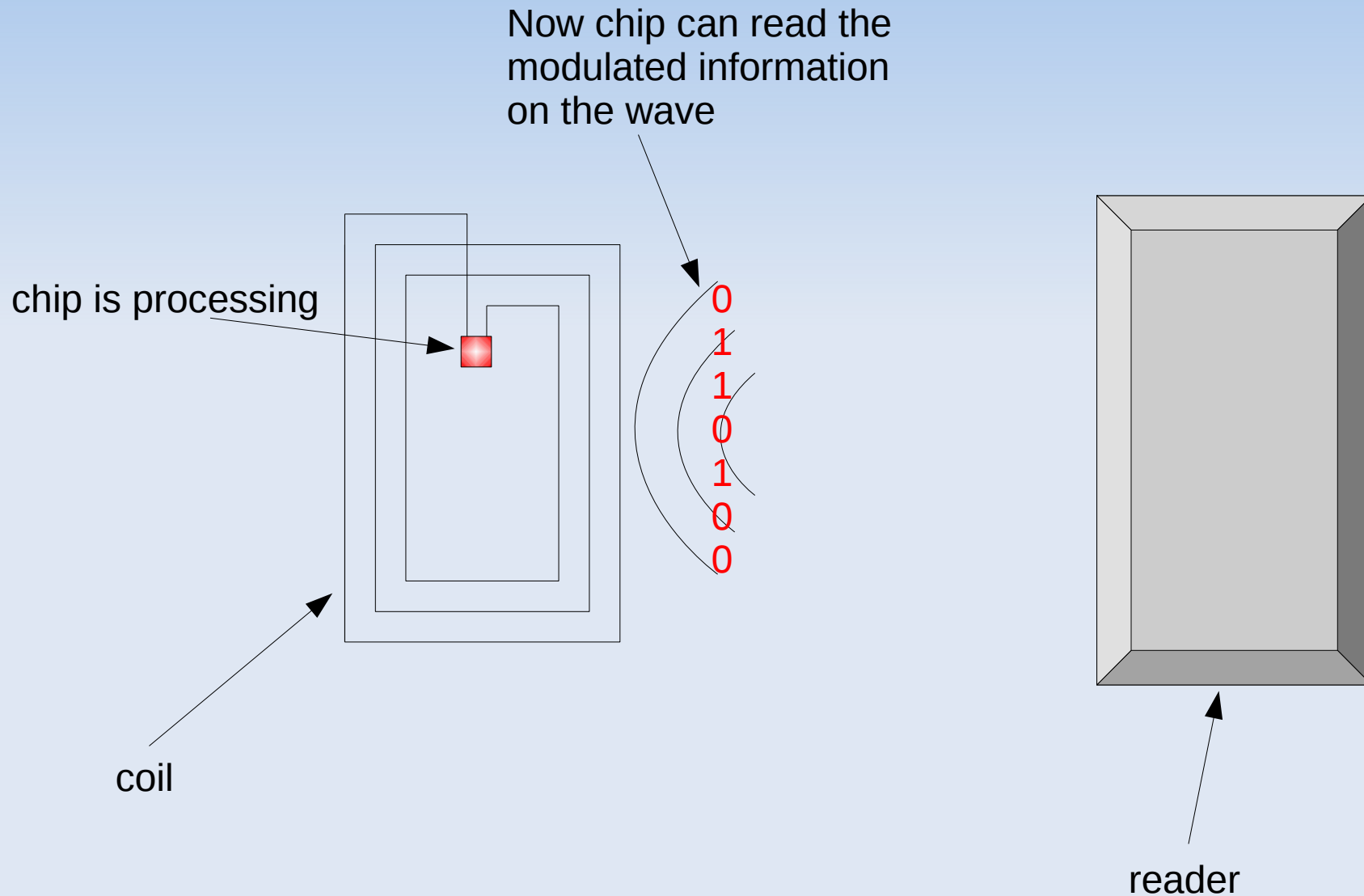
# How it works?



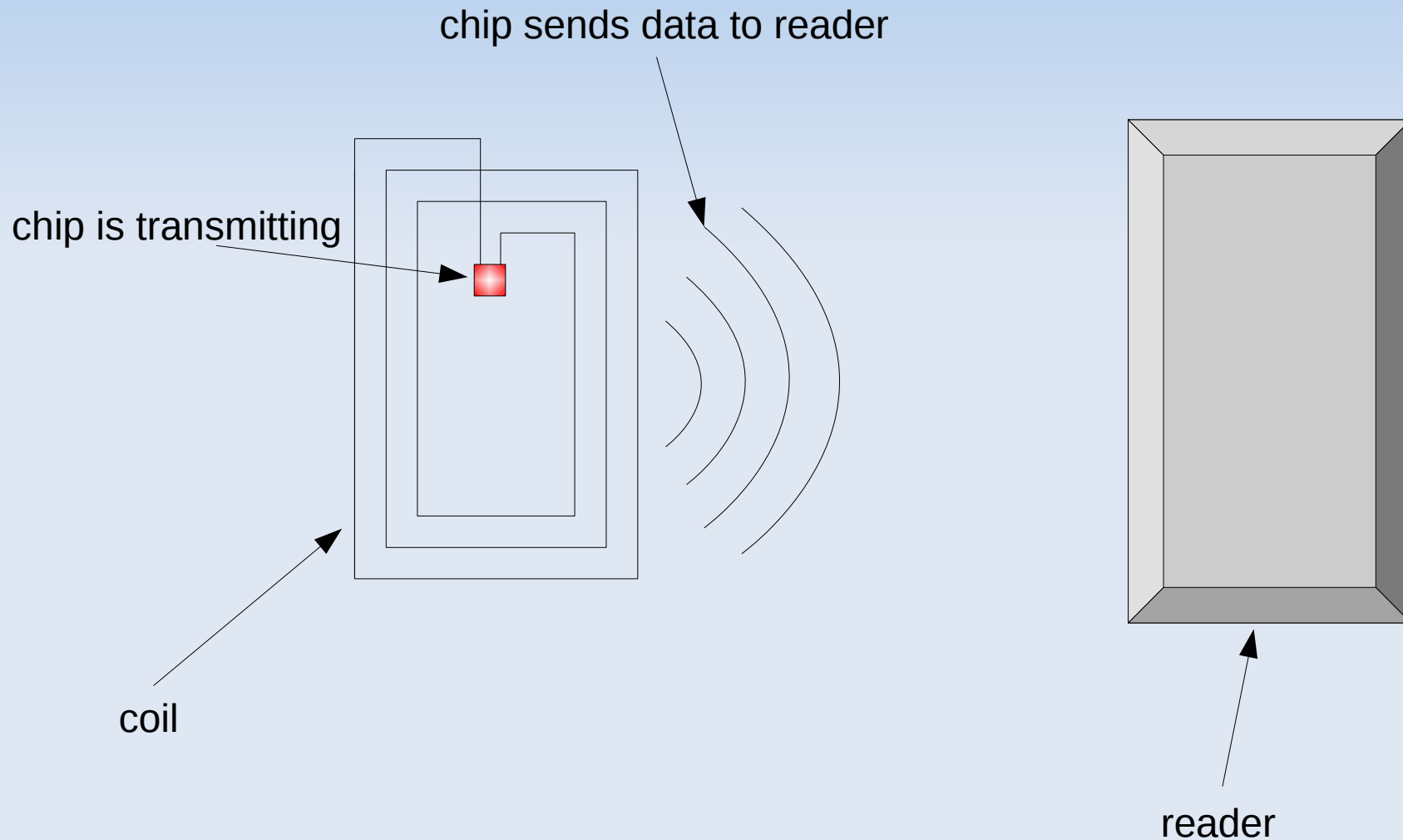
# How it works? (cont.)



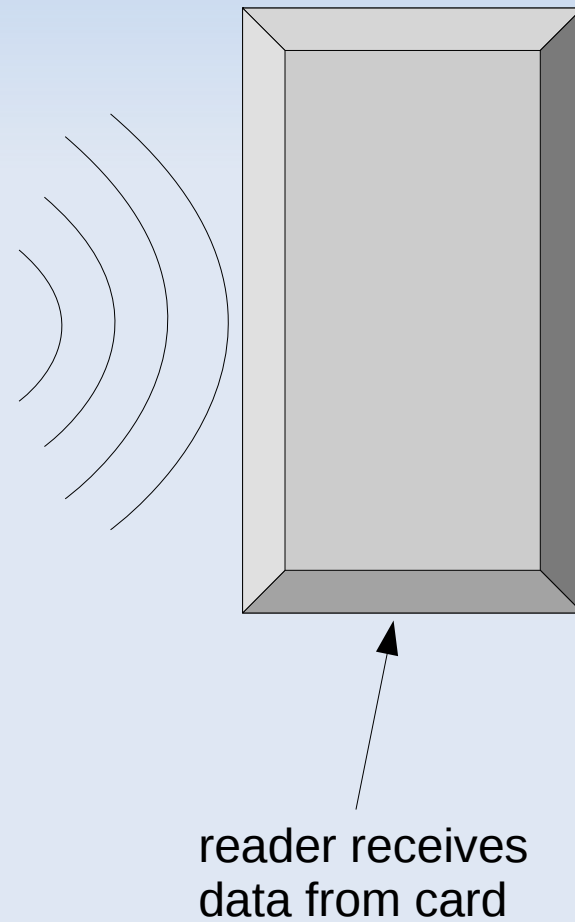
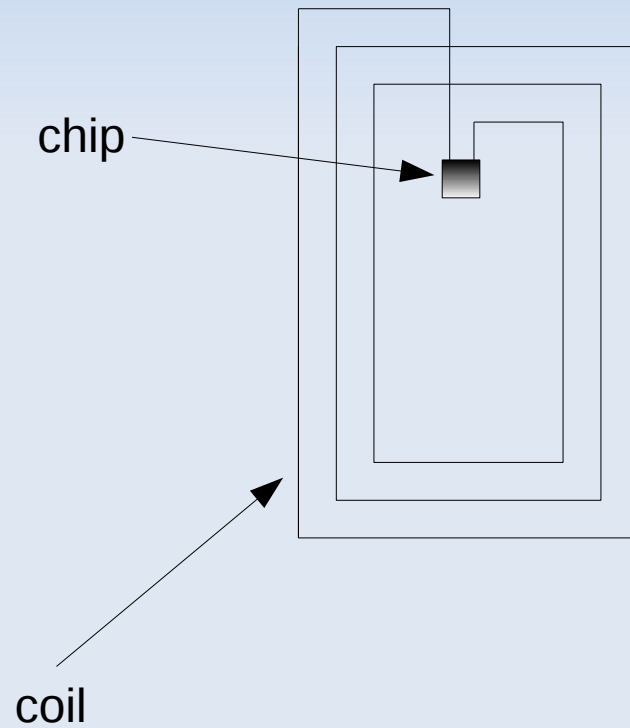
# How it works? (cont.)



# How it works? (cont.)



# How it works? (cont.)



# Mifare EEPROM Overview

- 1Kbyte, organized in 16 sectors with 4 blocks of 16 bytes each (16 byte per block);
- Allow access control for each block;
- The last block of each sector is called “trailer”, it contains 2 secret keys and access conditions;
- Data retention of 10 year;
- Write endurance 100.000 cycles.



# Mifare EEPROM Layout

Sector	Block	Byte within block
0	0	
	1	
	2	
	3	
1	0	
	1	
	2	
	3	
...	...	
15	0	
	1	
	2	
	3	

# Trailer Block (4<sup>th</sup> block each sector)

