IoT Security

Spring 2024

Karel Slavicek
Vaclav Oujezsky
Bacem Mbarek
Tomas Pitner

Outline

- Smart cards
  - History
  - Protocols
  - Utilization
  - Hardware

Smart card types

- Memory cards
- Crypto cards

- Contact cards
- Contactless cards

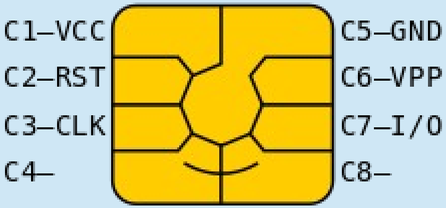
Contact smart cards

- SIM (Subscriber Identity Module)
- Bank cards
- Pre-payed telephone cards

Contact smart cards

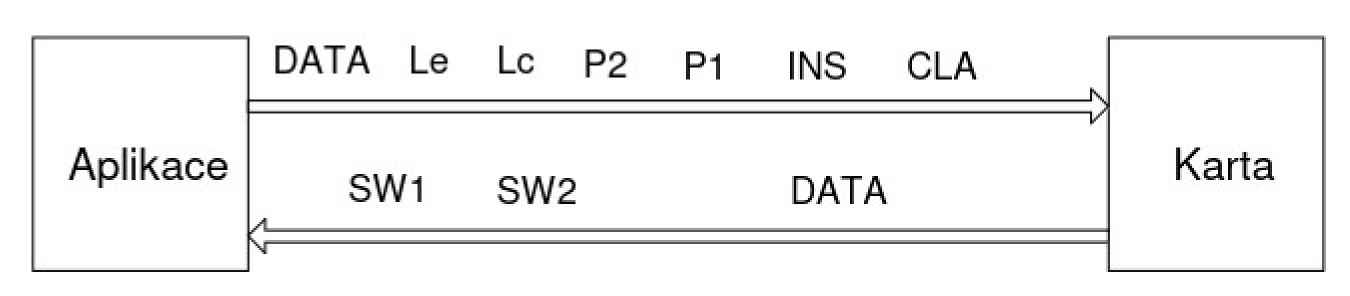
- Standards ISO/IEC 7816:
  - ISO 7816-1 - Physical characteristics: dimesions, thicness, flexibility, ...
  - ISO 7816-2 – chip and contacts locations, ...
  - ISO 7816-3 – Electrics parameters: volatage, current, ...
  - ISO 7816-4 – communication protocol,

    APDU, ...



APDU

- Application Protocol Data Unit



- CLA – Instruction class: 0x00 standard, 0x08 proprietary
- INS – Instruction code
- P1, P2 – Instruction parameters
- Lc – Instruction data length
- Le – Expected response data length
- DATA – Data
- SW1, SW2 – Return codes

Contactless smart cards

- ISO/IEC 14443:
  - ISO/IEC 14443-1:2018 Part 1: Physical characteristic
  - ISO/IEC 14443-2:2020 Part 2: Radio frequency power and signal interface
  - ISO/IEC 14443-3:2018 Part 3: Initialization and anticollision
  - ISO/IEC 14443-4:2018 Part 4: Transmission protocol
- ISO/IEC 15693 for longer distances

Contactless smart cards

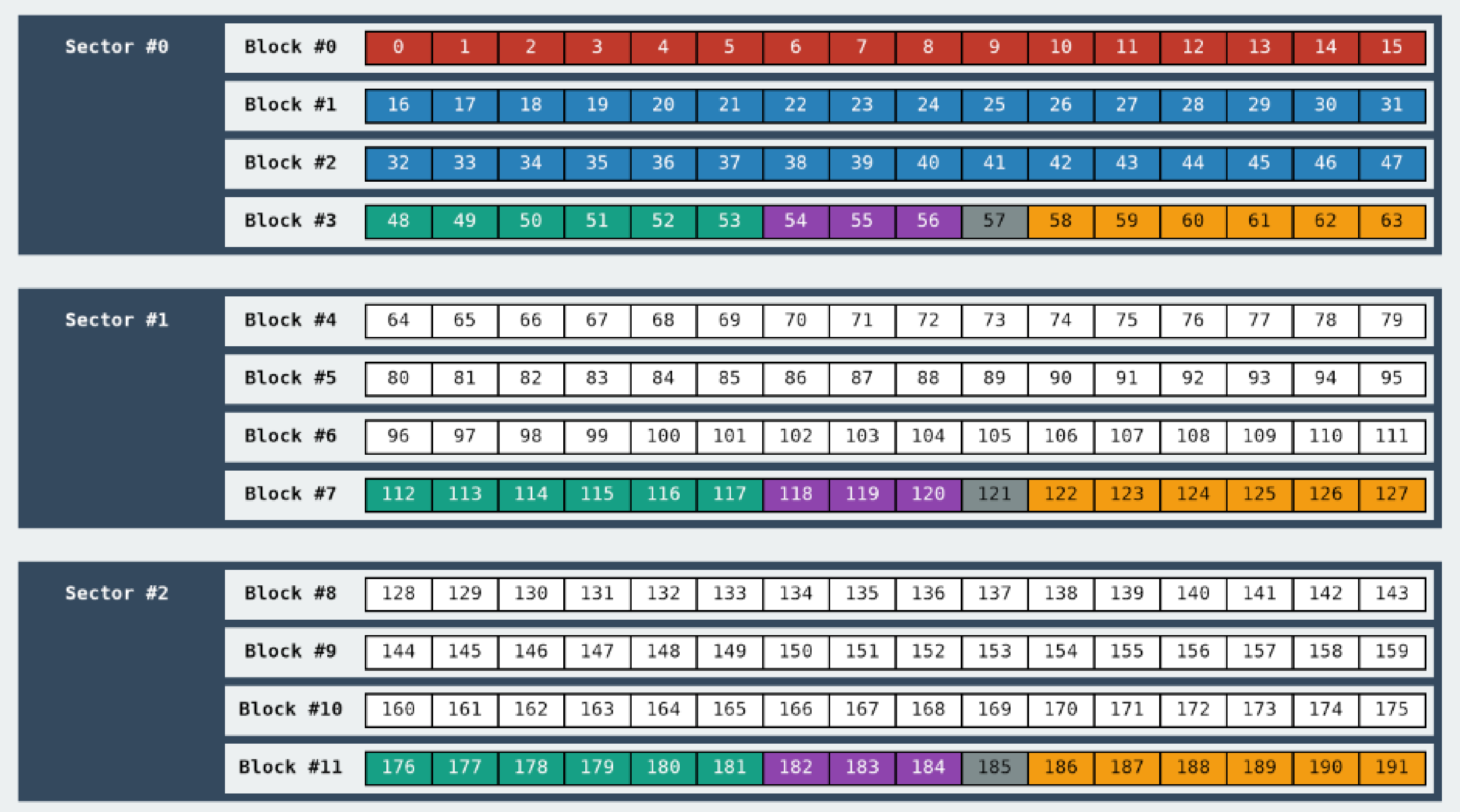
- RFID (Radio Frequency Identification)
- Arbitrary frequency and distance

- Low Frequency = 125 kHz – original RFID
- High Frequency = 13.56 MHz – NFC - proximity
- Ultra High Frequency = 868 MHz + 2.4 GHz – industrial applications

Smart card – data organization

- Sectors of 4 Blocks
- Each block = 16 bytes
- Number of blocks according to memory size
- First block: Manufacturer data
  - 4B / 7B UID
  - Rest of block proprietary
  - Read only

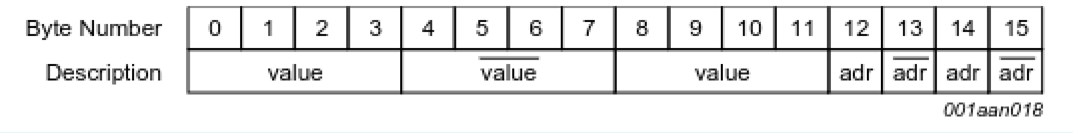
Smart card – data organization



Sector #0	Block #0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	Block #1	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	Block #2	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
	Block #3	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
Sector #1	Block #4	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
	Block #5	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
	Block #6	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
	Block #7	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
Sector #2	Block #8	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143
	Block #9	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
	Block #10	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175
	Block #11	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191

Smart card – data organization

- MIFARE Classic EV1:
  - read/write block
  - Value block
- Value Block (1 and 2 in sector 0, 0-3 otherwise)
- 4 Byte value, stored 3 times, once complementary
- Address 1-Byte, stored 4 times

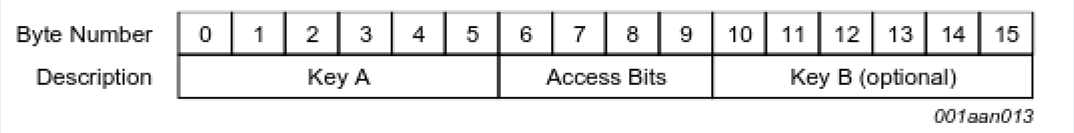


Byte Number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Description	value				$\overline{\text{value}}$				value				adr	$\overline{\text{adr}}$	adr	$\overline{\text{adr}}$

001aan018

Smart card – data organization

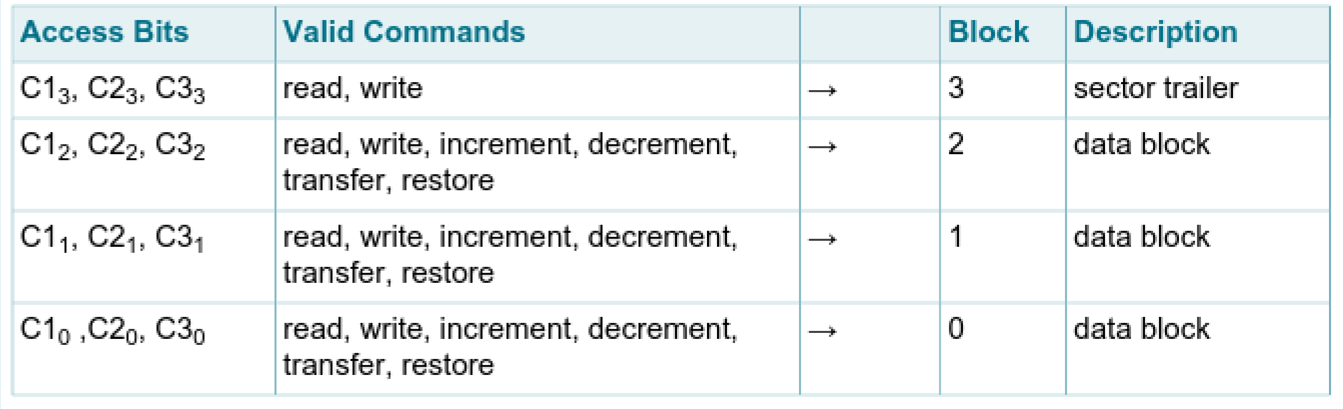
- Trailer block



Byte Number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Description	Key A						Access Bits				Key B (optional)					

001aan013

- Access Bits:



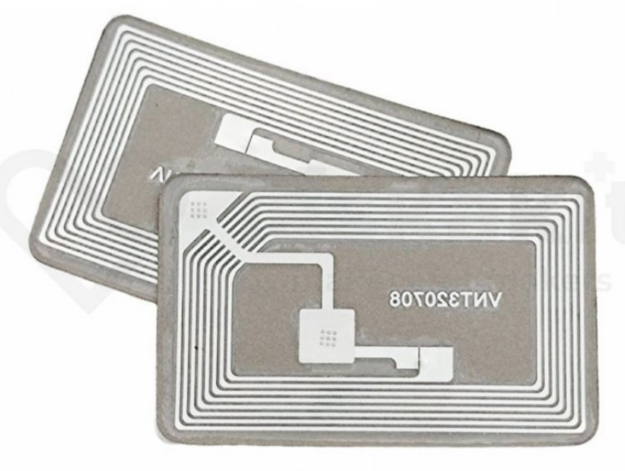
Access Bits	Valid Commands		Block	Description
$C1_3$, $C2_3$, $C3_3$	read, write	→	3	sector trailer
$C1_2$, $C2_2$, $C3_2$	read, write, increment, decrement, transfer, restore	→	2	data block
$C1_1$, $C2_1$, $C3_1$	read, write, increment, decrement, transfer, restore	→	1	data block
$C1_0$,$C2_0$, $C3_0$	read, write, increment, decrement, transfer, restore	→	0	data block

Smart card – Memory operations

Operation	Description	Block type
Read	reads one memory block	read/write, value, and sector trailer
Write	writes one memory block	read/write, value, and sector trailer
Increment	increments the contents of a block and stores the result in the internal Transfer Buffer	value
Decrement	increments the contents of a block and stores the result in the internal Transfer Buffer	value
Transfer	writes the contents of the internal Transfer Buffer to a block	read/write, value
Restore	reads the contents of a block into the internal Transfer Buffer	value

Hardware

- Main smart cards manufacturer: NXP
  - MIFARE
  - NTAG213/215/216



- Main card readers manufacturer: NXP
  - RC522 (MFRC522)
  - PN532

MIFARE

- MIFARE Classic - Proprietary protocol compliant with ISO/IEC 14443 1-3 Type A, NXP proprietary security protocol Crypto1

  Subtypes: MIFARE Classic EV1

- MIFARE Plus - Replacement for MIFARE Classic with cAES-128 based security, backwards compatible with MIFARE Classic.

  Subtypes: MIFARE Plus S, MIFARE Plus X, MIFARE Plus SE and MIFARE Plus EV2.

- MIFARE Ultralight - Low-cost solution for high volume applications (public transport, loyalty cards, event ticketing)

  Subtypes: MIFARE Ultralight C, MIFARE Ultralight EV1, MIFARE Ultralight Nano and MIFARE Ultralight AES.

- MIFARE DESFire - Compliant with parts 3 and 4 of ISO/IEC 14443-4 Type A. Mask-ROM operating system from NXP.

  Subtypes: MIFARE DESFire EV1, MIFARE DESFire EV2, MIFARE DESFire EV3 and MIFARE DESFire Light.

MIFARE Competitors

- HID Global :
  - iCLASS
  - MIFARE DESFire EV3
  - HITAG
- SONY :
  - FeliCa – mainly in Japan

Thank for your attention!

Questions and comments?