

EE 4215

Security Technology

Lecture 9: Smart-card Security
2018/19 Semester B

Course Structure

- Week 1: Security Fundamental
- Week 2: Classical Cryptography
- Week 3: Number Theory &
- Week 4: DES
- Week 5: Secret-key Cryptography
- Week 6: Public-key Cryptography
- Week 7: Quiz 1
- Week 8: Hashing, Digital Signature, PKI
- Week 9: SSL/TLS, Web Security
- Week 10: Wi-Fi & P2P Security
- Week 11: Smart-card Security
- Week 11: Quiz 2
- Week 12: Cloud Computing Security
- Week 13: Blockchain Security, Secure-code, Trusted Hardware, Review

Lecture 9: Smart-card Security

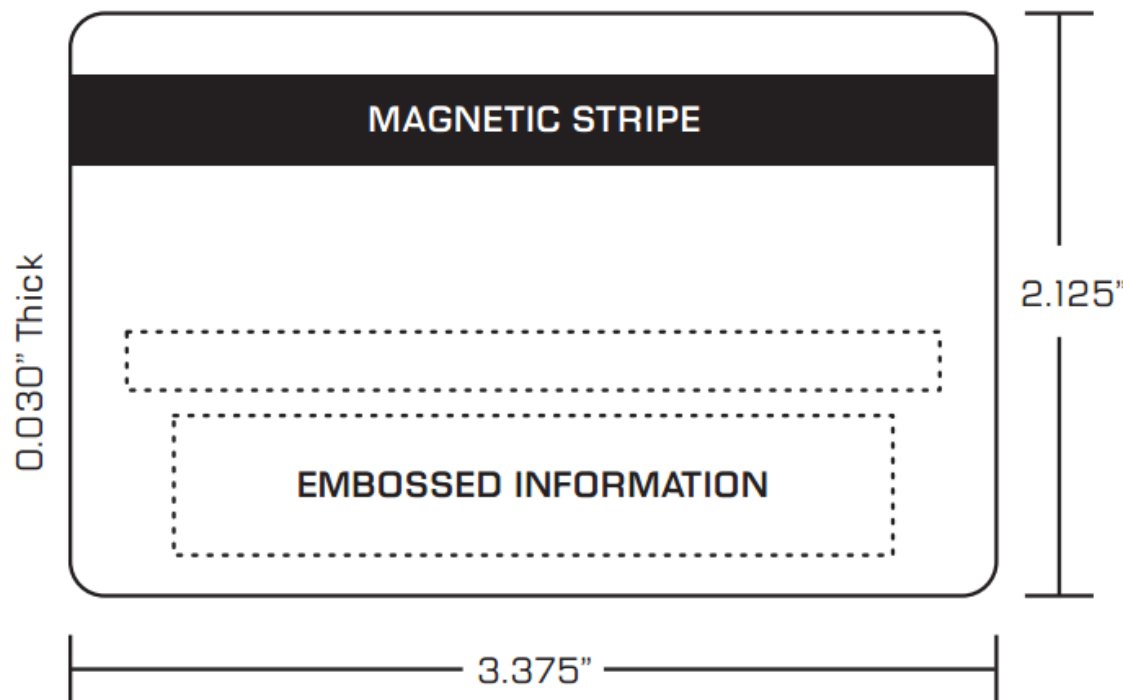
- Magnetic Card
- Smart Card
- RFID
- Mifare Classic Card

Card Era

- Cards are commonly used in our daily life
 - Bank ATM card
 - Credit card
 - Octopus card
 - Membership cards, door entrance cards, etc
- Technology
 - Magnetic card vs smart card

Magnetic Card

- composed of a layer of magnetic material for storing information
- maximum 3 stripes / tracks



ISO

7810	Physical characteristics of credit card size document
7811-1	Embossing
7811-2	Magnetic stripe - low coercivity
7811-3	Location of embossed characters
7811-4	Location of tracks 1 & 2
7811-5	Location of track 3
7811-6	Magnetic stripe - high coercivity
7813	Financial transaction cards

Magnetic Strips

- Track 1 is developed by International Air Transportation Association (IATA)
 - contains adaptive 6-bit alphanumeric characters
- Track 2 is used by American Bankers Association (ABA)
 - stores 4-bit numerical information containing identification number and control information.
- Track 3 is originated by Thrift Industry
 - contains information which is intended to be updated with each transaction

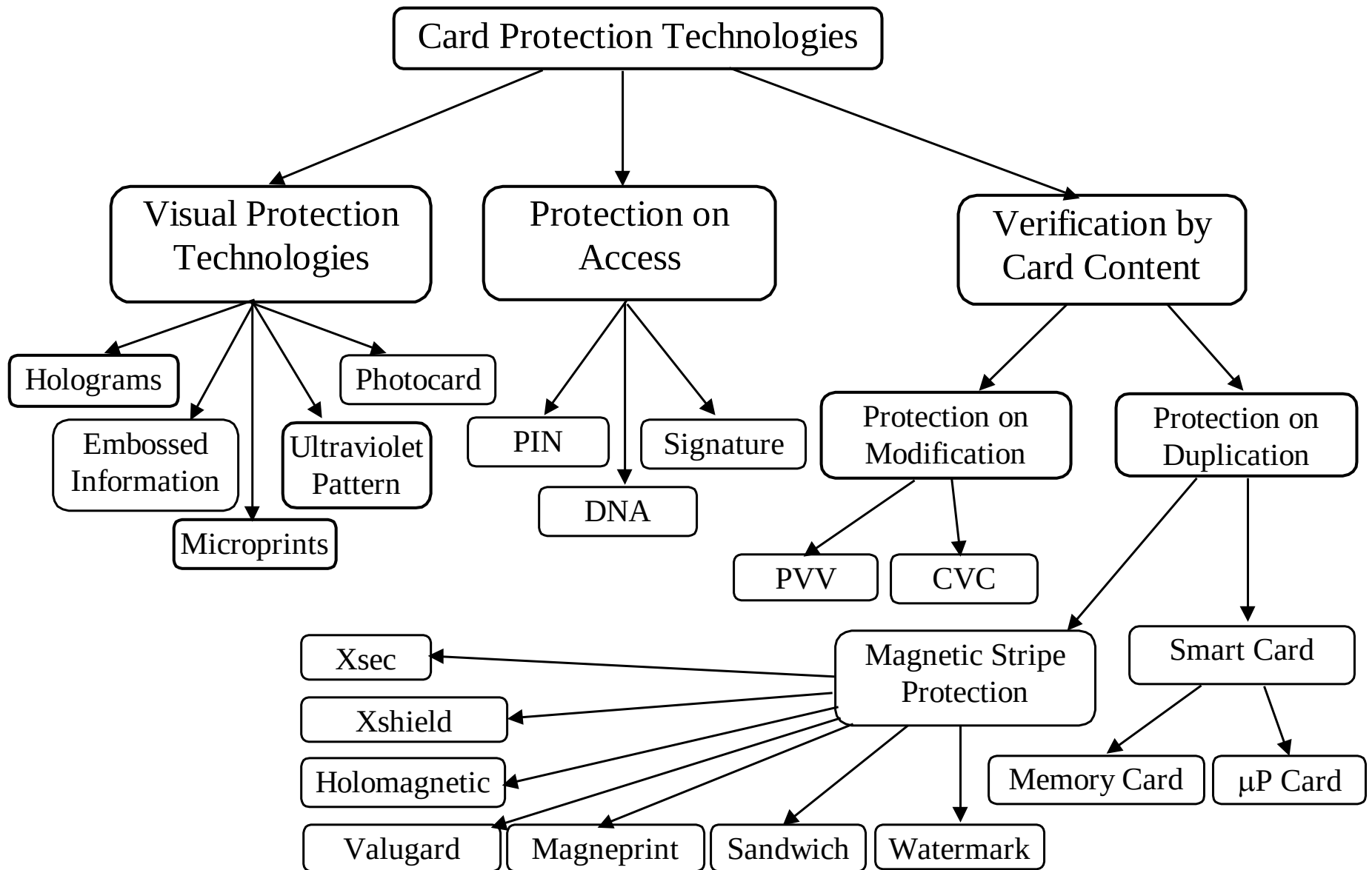
0.223" ↑ ↓	Track		Recording Density	Character Configuration	Information Content
			(bits per inch)	(including parity bit)	(including control characters)
0.110"	1	IATA	210	7 bits per character	79 alphanumeric characters
0.110"	2	ABA	75	5 bits per character	40 numeric characters
0.110"	3	THRIFT	210	5 bits per character	107 numeric characters

Fraud Activities

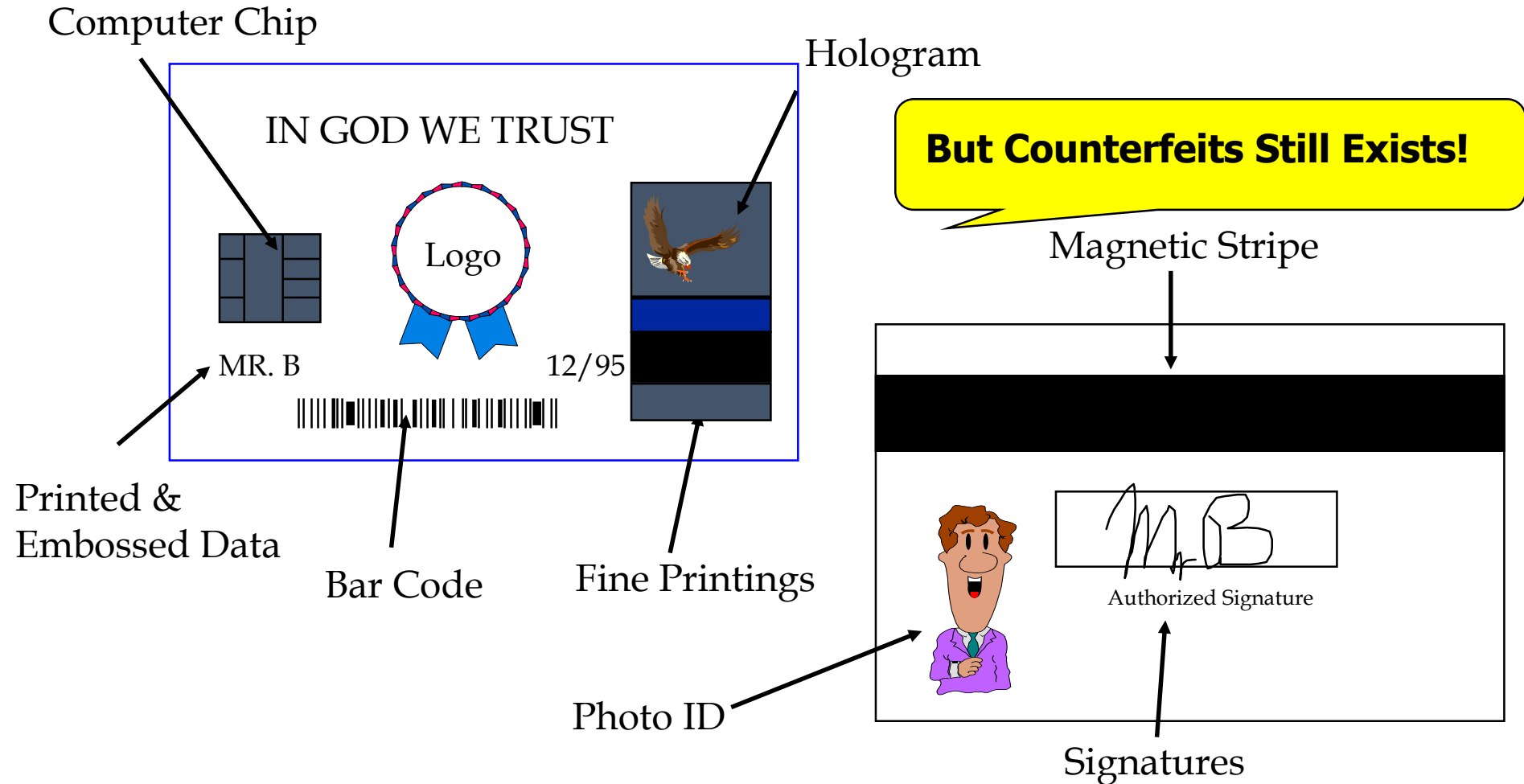
- **Stealing**
 - Steal a legal card
- **Altering** and **re-embossing** a genuine card
 - modify the visual features of card.
- **Skimming**
 - copy the original electronic data stored on the magnetic stripe
 - commonly used in credit card fraud
- **Buffering**
 - re-encoding the original data to the magnetic card
 - commonly used in producing card counterfeits of store-value ticket.

Card Protection Technologies

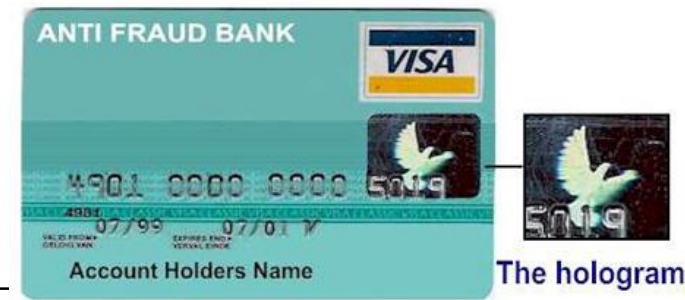
- Validation by Appearance
 - visual mean to protect against illegal duplication
 - make the appearance of card so unique and difficult to duplicate that shopkeepers or card handlers can identify the genuine card instantly
- Verification on Access
 - relies on the interaction with the card holder, to identify the person accessing the card is an authorized one
 - e.g. requires user to input PIN



Validation by Appearance



Holograms



- The most notable marking for credit cards
 - produced by a combination of photography and laser beams
 - initially counterfeit holograms were crude and manufactured by stamping tin foils
 - recently counterfeit holograms require professional technical knowledge to validate the authenticity of holograms

Embossed Characters

- Some raised marks implemented on the plastic surface of card
- The embossed information includes
 - user name, expiry date, card number and unique embossed symbol, etc
- However, the card material is a thermal plastic
 - by warming the card to about 50°C, it allows “debossing” of the characters and re-embossing with fraud information

Photocards

- introduced by CitiBank Corporation
- the effectiveness of photocard on marketing purposes seem to be greater than that on security
- it is not an effective mean to stop card fraud because counterfeiters had the ability to imitate laser engraved photographs and signatures in rather low cost using a photomachine at around US\$5,000.

Protection on Card Access

- Card holder is requested to prove his identity
 - Card itself – authentication by “What you have”
- Common methods:
 - PIN - authentication by “What you know”
 - Provided by the issuer (e.g. bank)
 - Biometrics – authentication by “What you are”
 - Fingerprint, iris pattern, speed of writing, etc
 - accuracy is not 100%
 - Signature
 - most popular way of verification

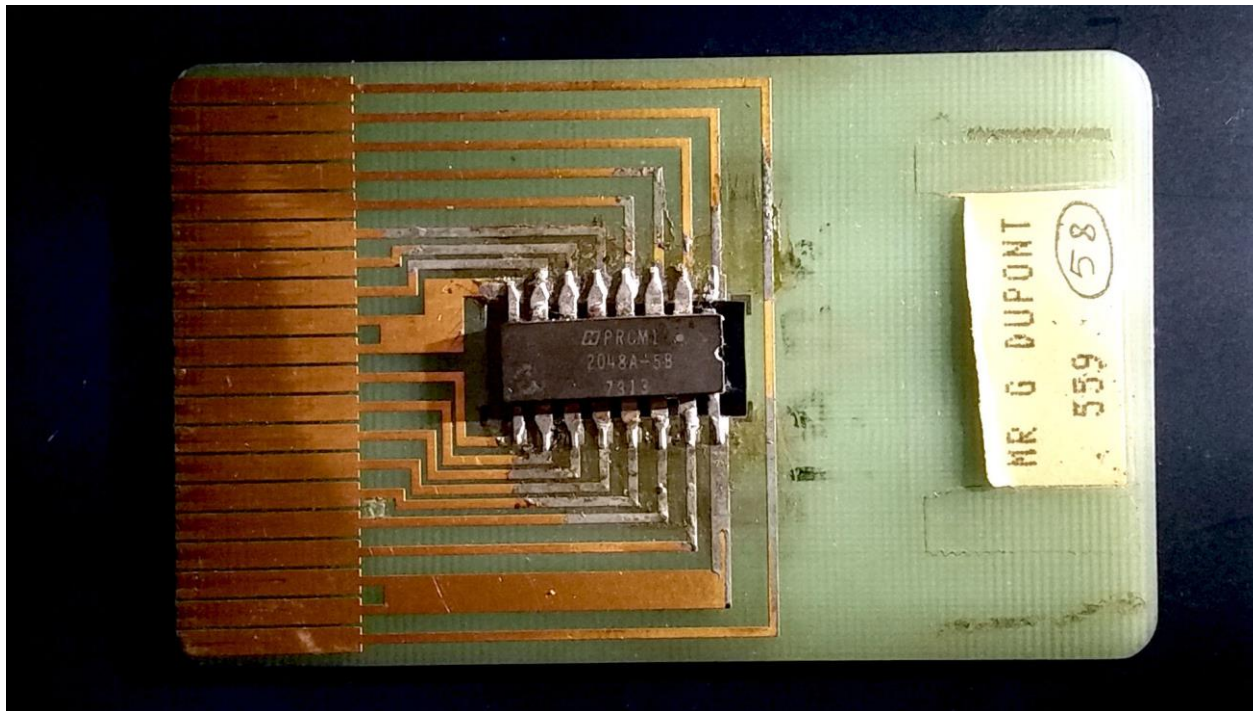
Smart Card

- Integrated Circuit - chip
 - originated from France
 - invented in 1970 and matured in 1990
- A replacement for magnetic card



Historical Smart Card

- Wikipedia: One of the first smart-card prototypes, created by its inventor Roland Moreno around 1975. We can see how each leg of the microchip is connected to the exterior world by a copper connector.



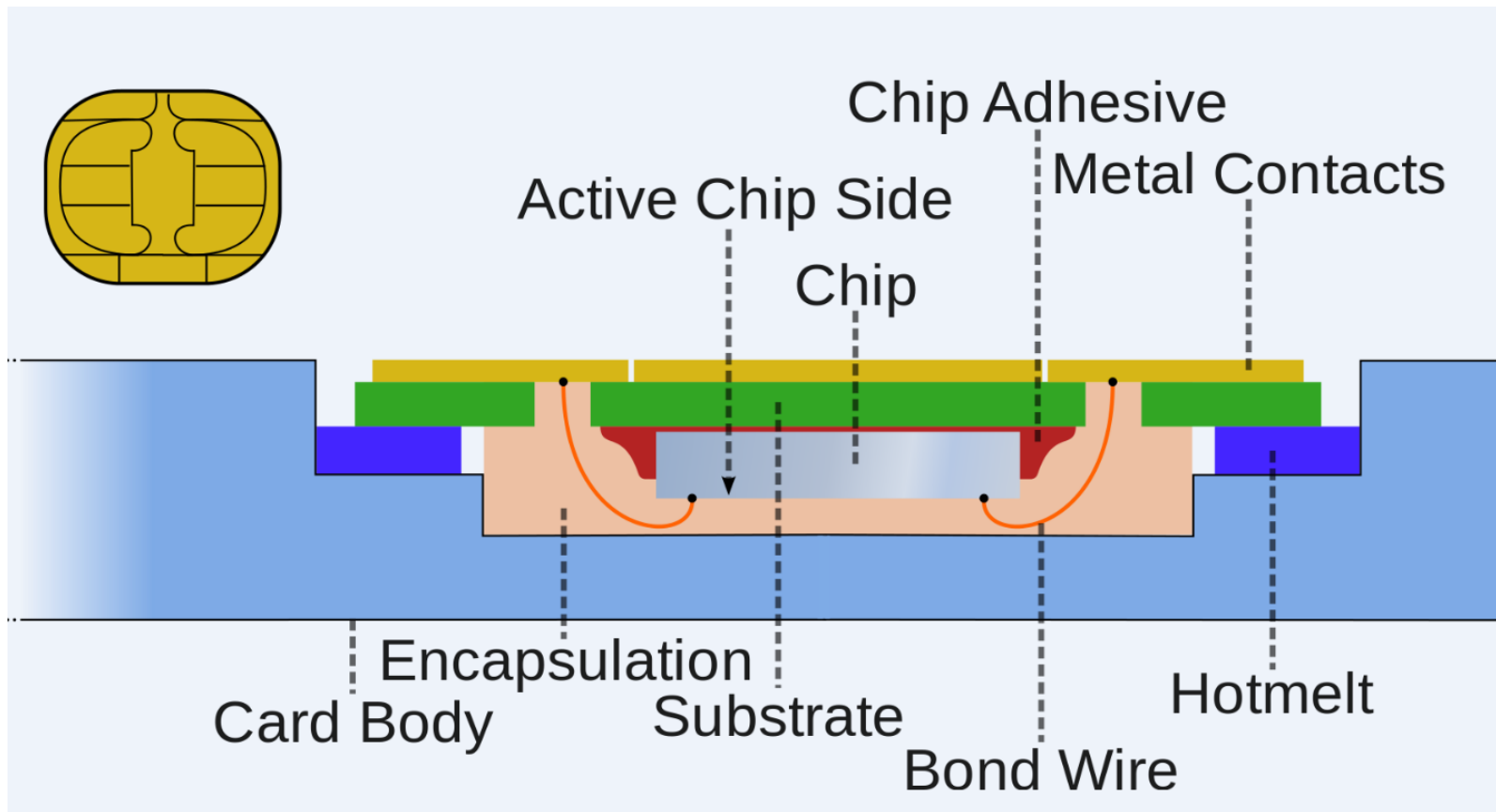
Contact Pads

- Different styles



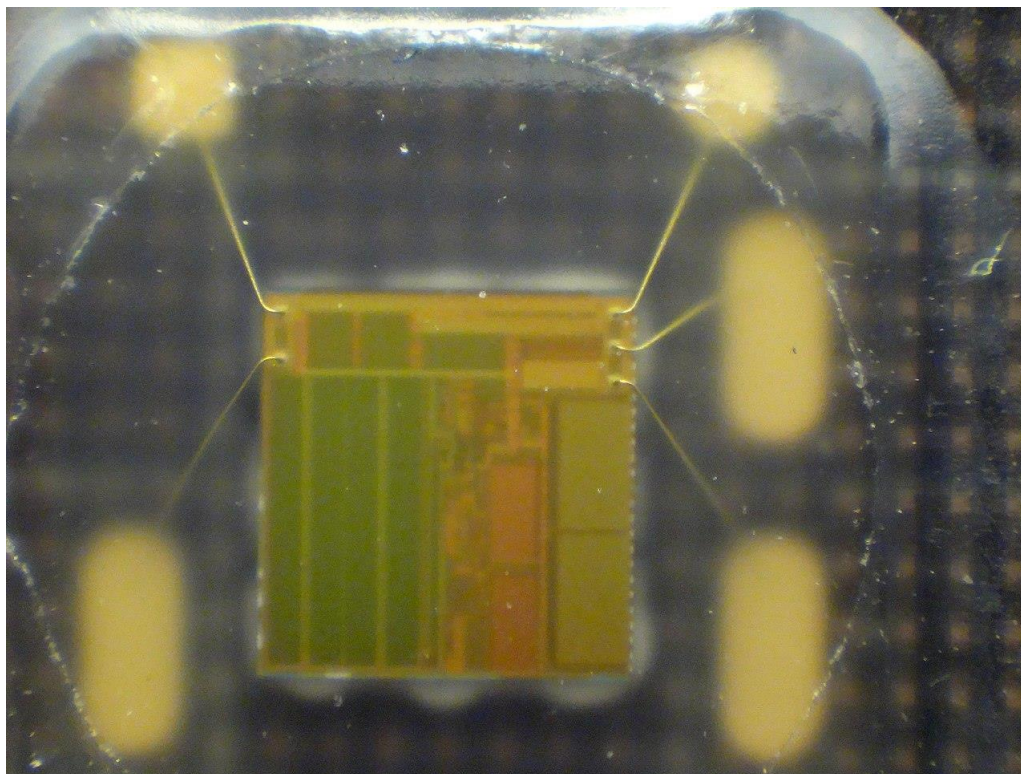
Packaging

- Where is the bond wire?



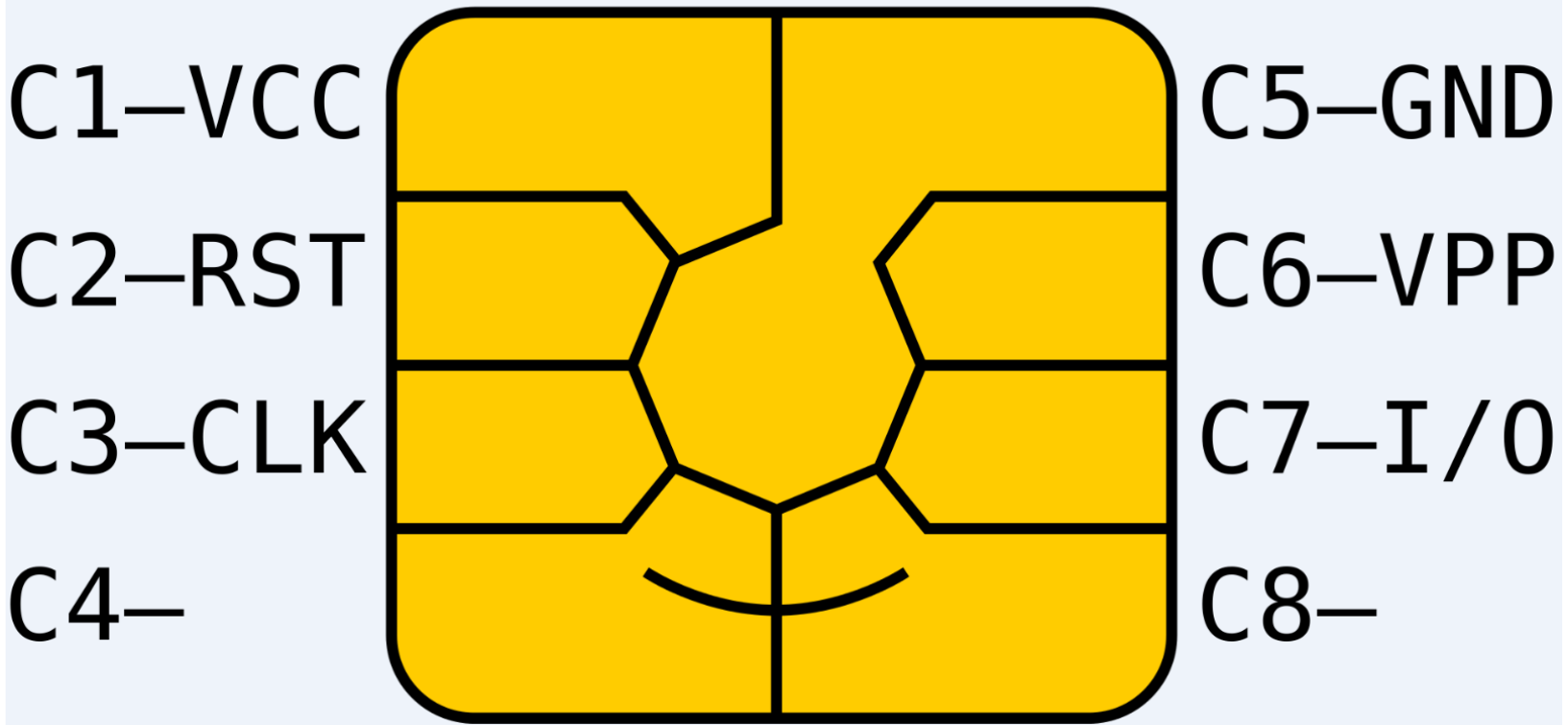
Golden Wire

- You can locate the golden wires inside the smart card.



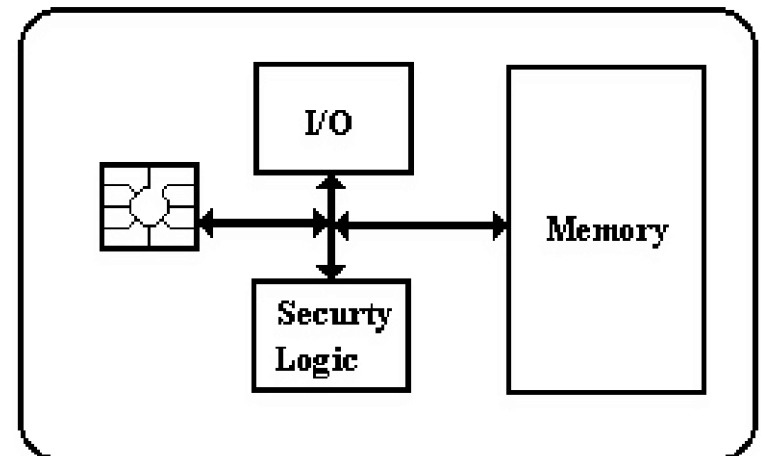
Contact Pad locations

- Follow the International ISO/IEC 7816-3:2006 Standard.
- <https://www.iso.org/standard/38770.html>



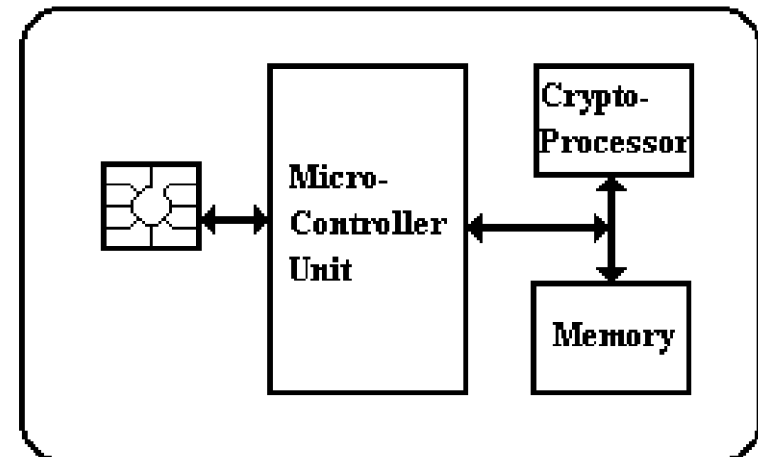
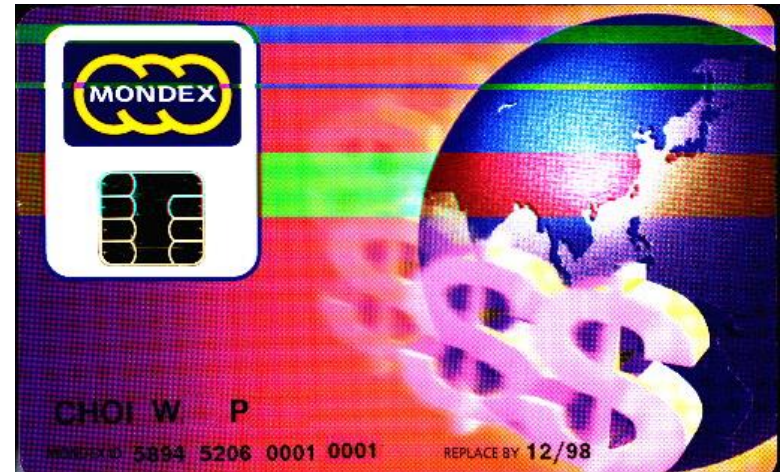
Memory Card

- Composed of EEPROM/PROM
- simple function, e.g. prepay card

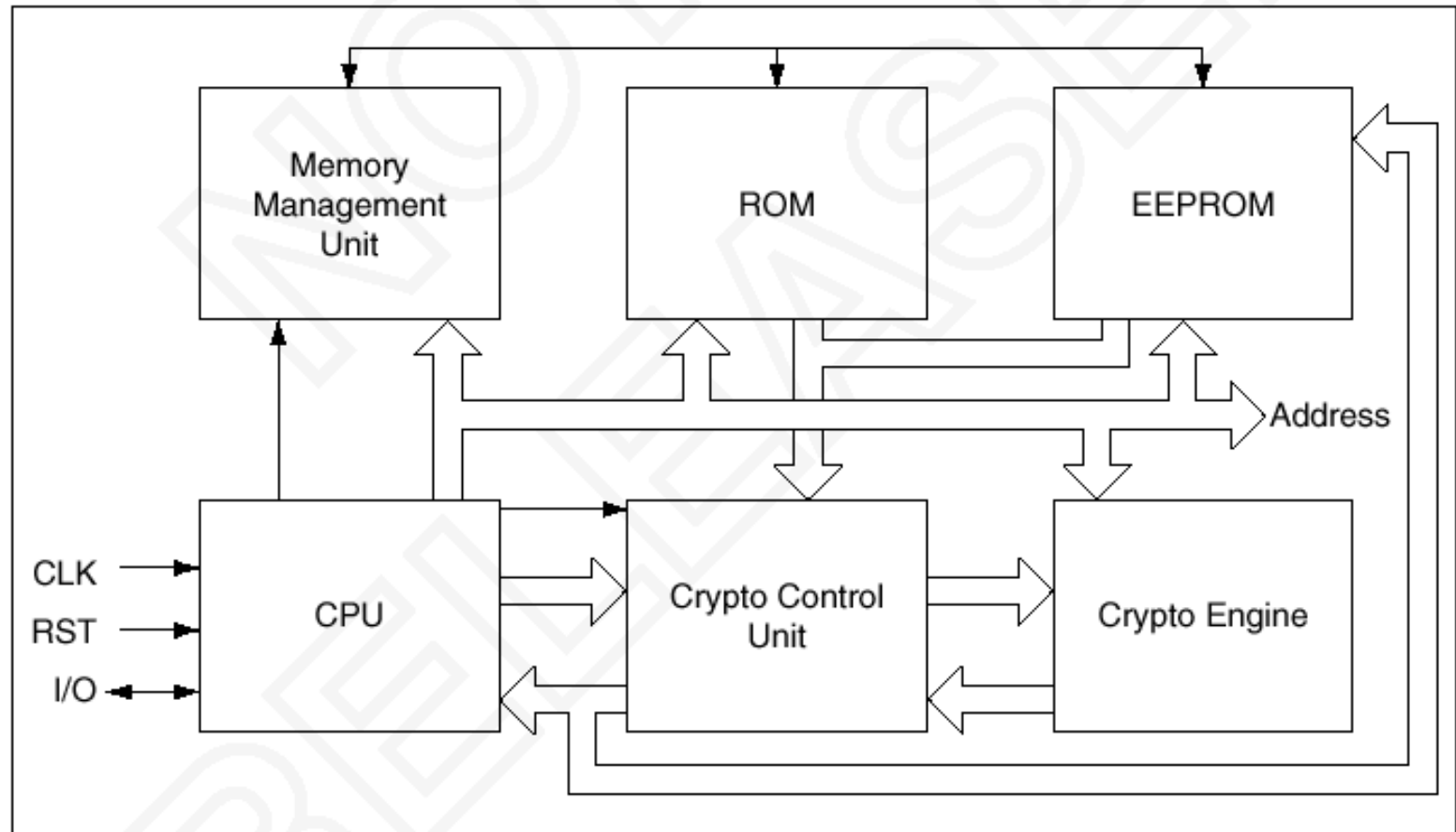


Crypto-processor IC Cards

- composed of crypto-processor & PROM
 - a powerful MPU
- can recognise illegal signal and have crypto capabilities



Basic Internal Structure of CPU Smart Card



Advantages of Smart Card

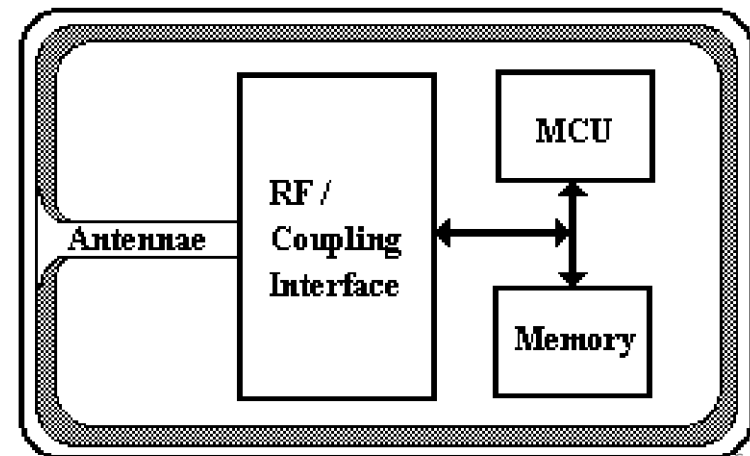
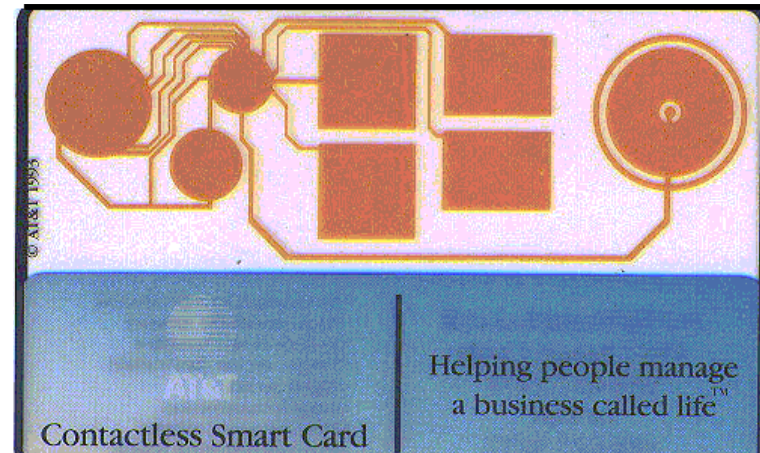
- Large storage capacity
- more security features
- multiple functions
- flexibility in use - intelligent, lower power consumption, effective packaging
- as access card, electronic purse, debit/credit cards, ID card etc.

Technologies

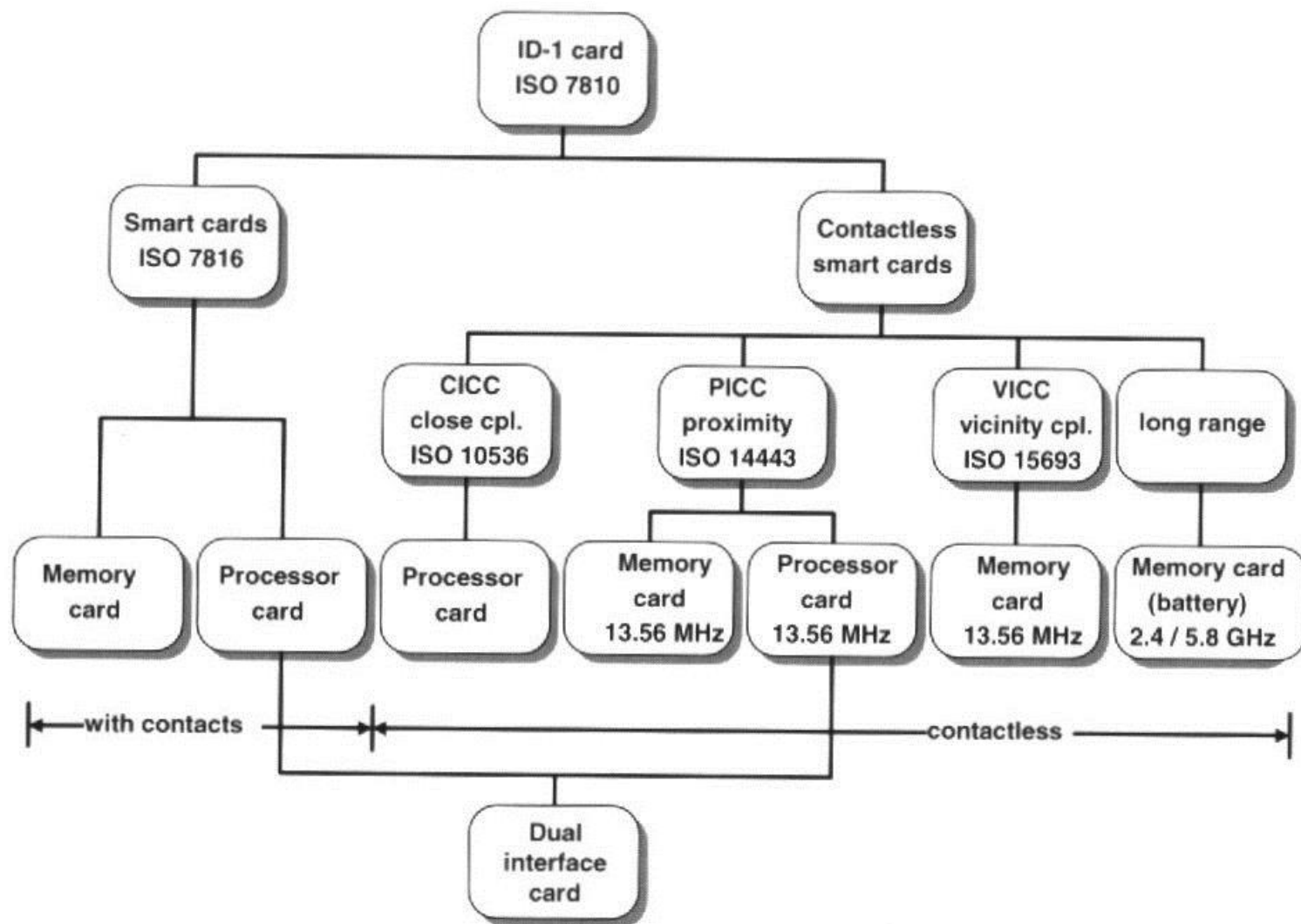
- Data Storage Management - information protection
- Encryption
 - AES, RSA, Elliptic Curve Cryptography, etc
- Additional Authentication
 - biometric: fingerprint, facial features, iris identification, dynamic signature recognition, etc
- Open platforms are developed to support multiple applications
 - Multos (used in HKID smartcard)
 - Java card

Contactless Smart Card

- similar to contact smart card
- with RF transceiver to increase robustness and security



Standards



RFID

- RFID is an hybrid Application Specific Integrated Circuit (ASIC) mounted in a tag or label.
- It will send out a stream of pre-stored data when activates by a corresponding radio waves
- Potential replacement of barcodes

History of RFID Development

- First developed for missile tracking and telemetry in military applications
- Widely used in Animal Tracking in 80's
- Later for use in Parking and toll road payment
- Large scale use in Access Control for security systems
- Now for inventory tracking and logistic management

Advantages of RFID

- Can operate in severe conditions
- Can read through obstacles
- Unaffected by static charges
- Well protected from exposure

Wide Range of Applications

- Cargo Tracking
- Animal Tracking
- Inventory Tracking
- Baggage Tracking
- Children eye of sight alarming
- Access Control
- Road Toll/Parking payment
- Border entry for vehicle/driver identification

ISO Standards

- ISO 11784/85 short distance in 125KHz
- ISO 14443 short distance in 13.56 MHz frequency
- ISO 15693 long distance in 13.56 MHz frequency
- ISO 18000 covers various distances and frequency ranges <key development now>

Readers Available in Field



Short Range
Reader <10cm>



Mid Range
Reader <2m>



Long Range
Reader <10m>



Mid Range
Gate Antenna



Long Range
Panel Antenna



Extra Long Range
High Performance
Area Antenna

Tags Available in field

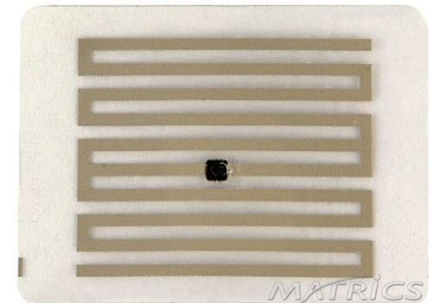
Long
Distance



Paper Label using in HK Airport

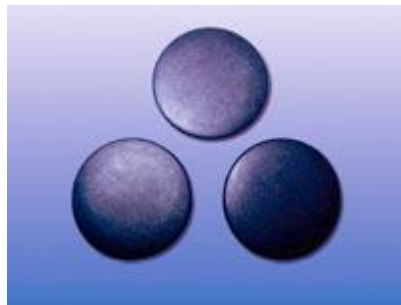


Concrete

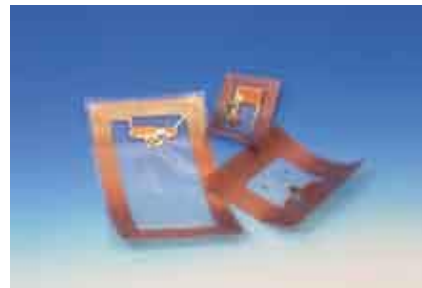


Glass

Short
Distance



Encapsulated Tag

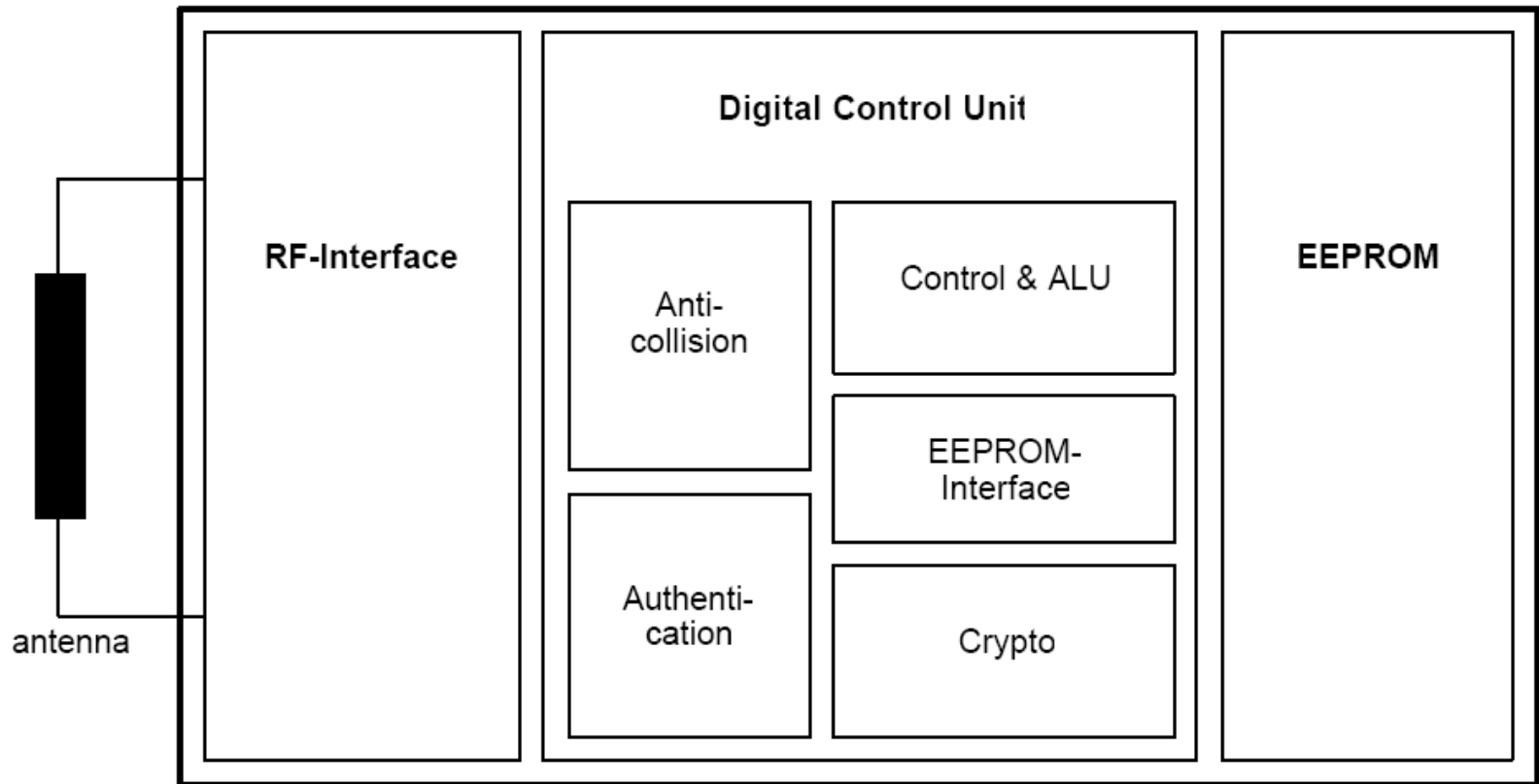


Label Inlay



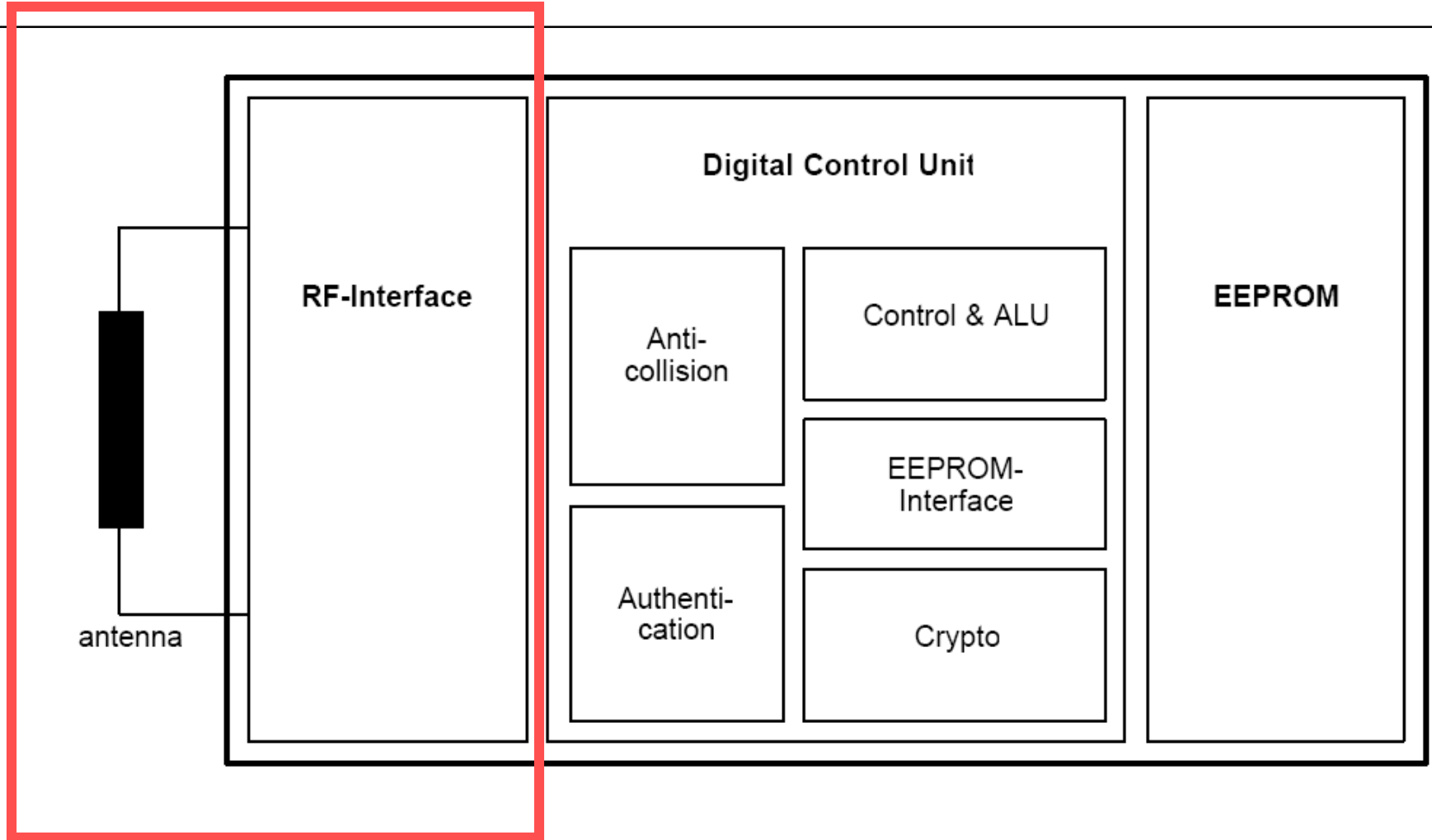
Glass
Encapsulated

Mifare Card MF1 IC S50 Architecture



Mifare Card MF1 IC S50 Architecture:

RF-Interface

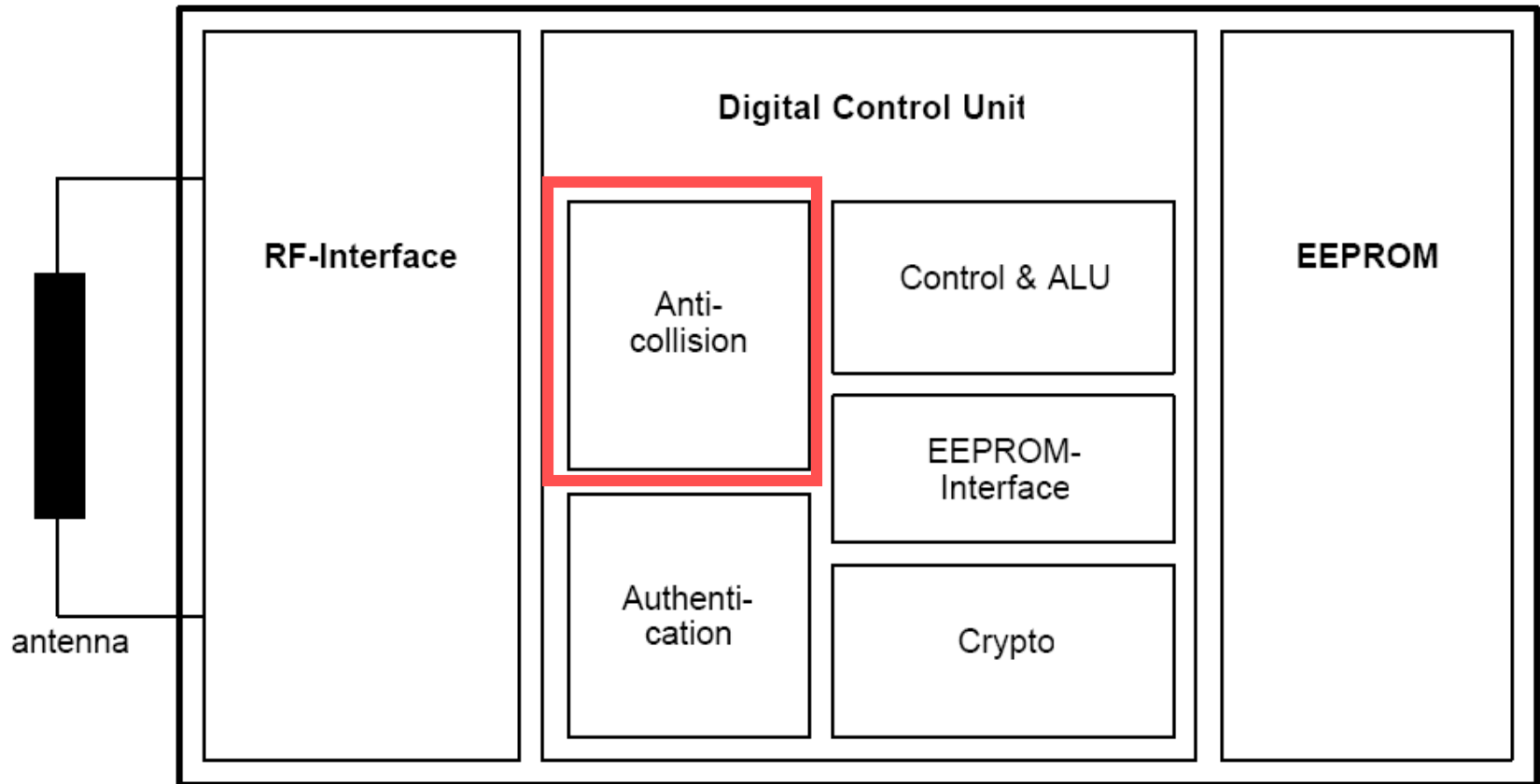


RF-Interface

- Modulator/Demodulator
- Rectifier
- Clock Regenerator
- Power On Reset
- Voltage Regulator

Mifare Card MF1 IC S50 Architecture:

Anticollision

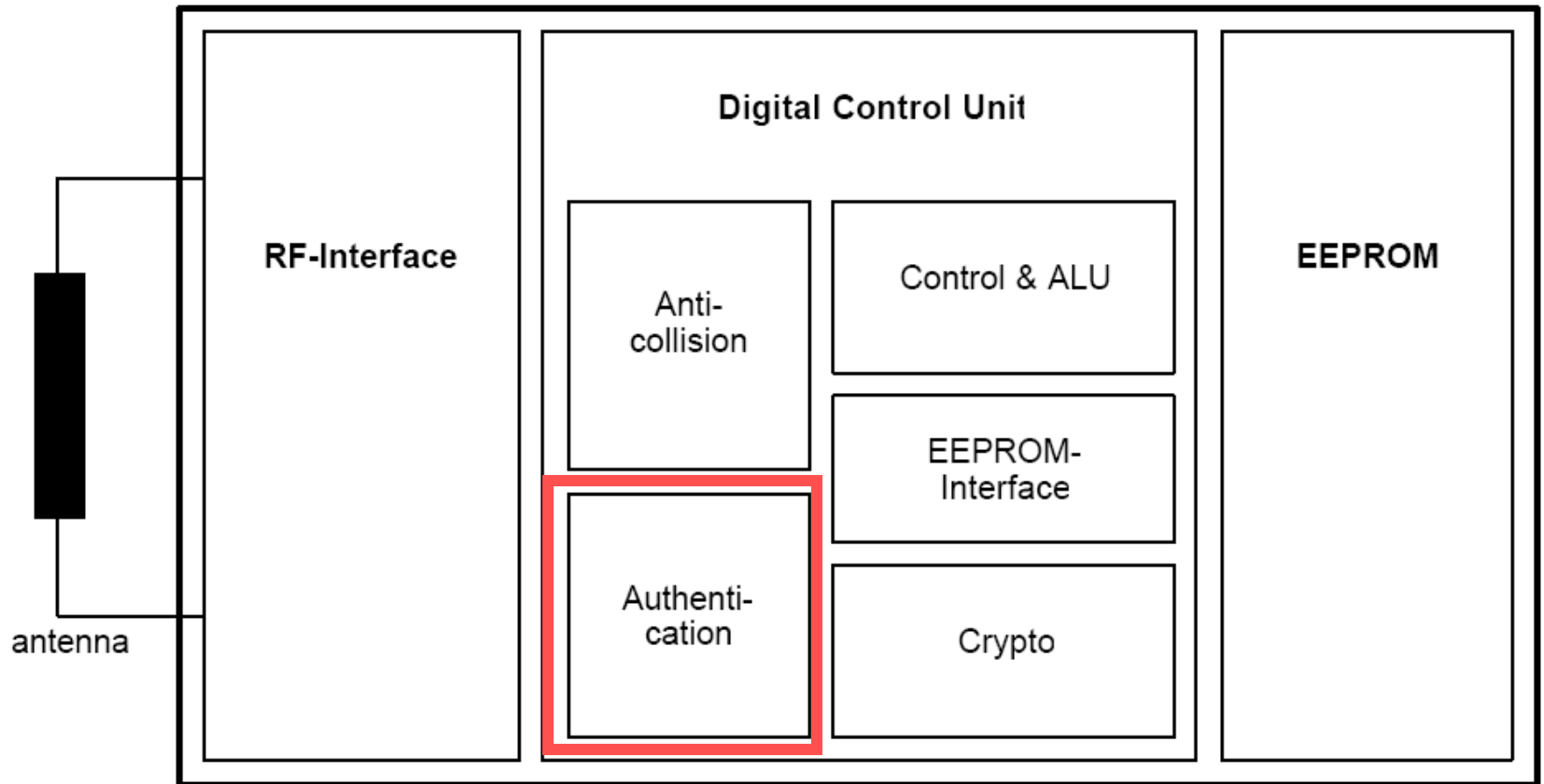


Anticollision

- To prevent collisions when multiple cards are presented in the same antenna field
- To select and operate each card in sequence

Mifare Card MF1 IC S50 Architecture:

Authentication

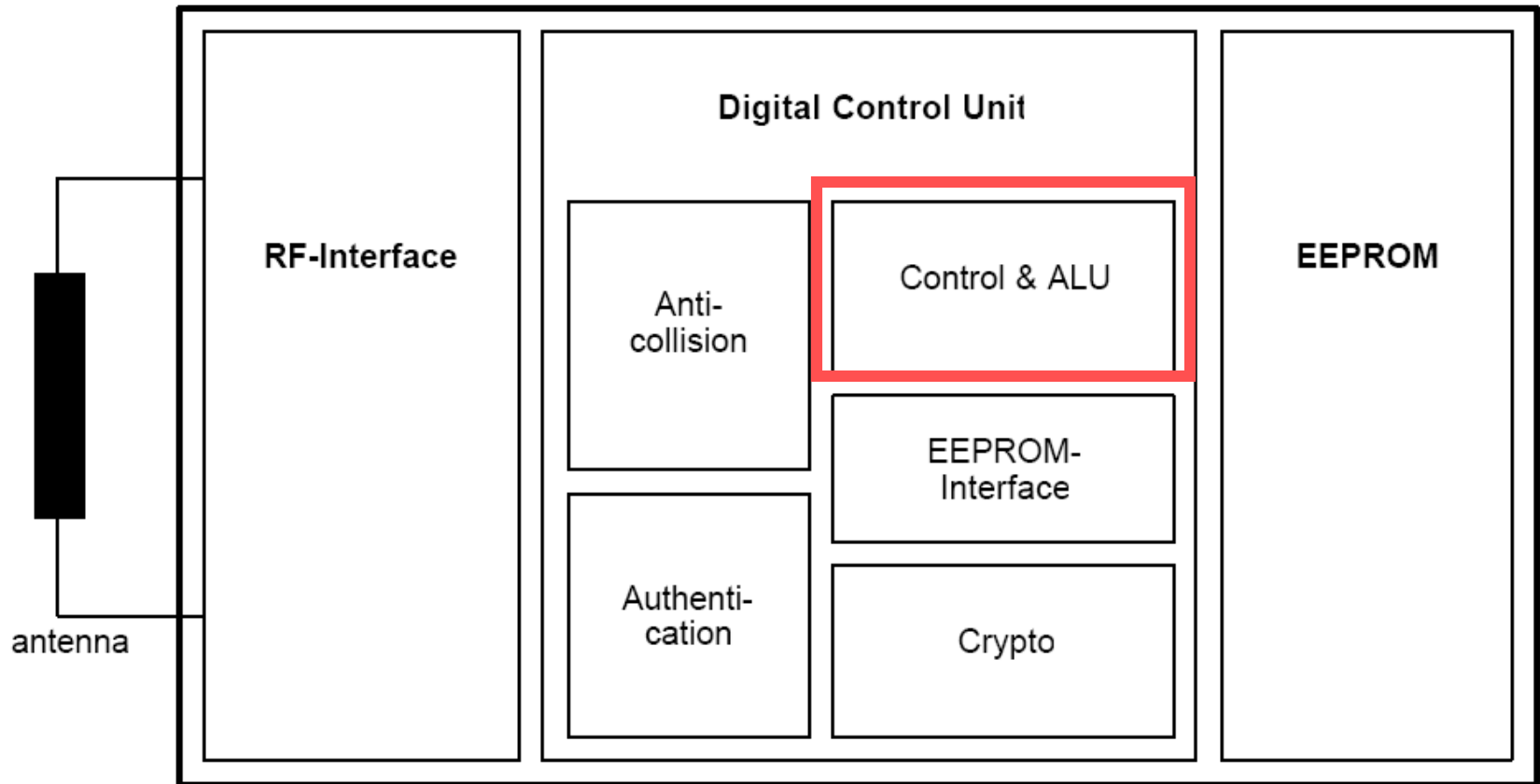


Authentication

- Must be done before any memory operation
- To ensure that access to a sector is only possible through the two keys (namely key A and key B) specified for each sector

Mifare Card MF1 IC S50 Architecture:

Control & ALU

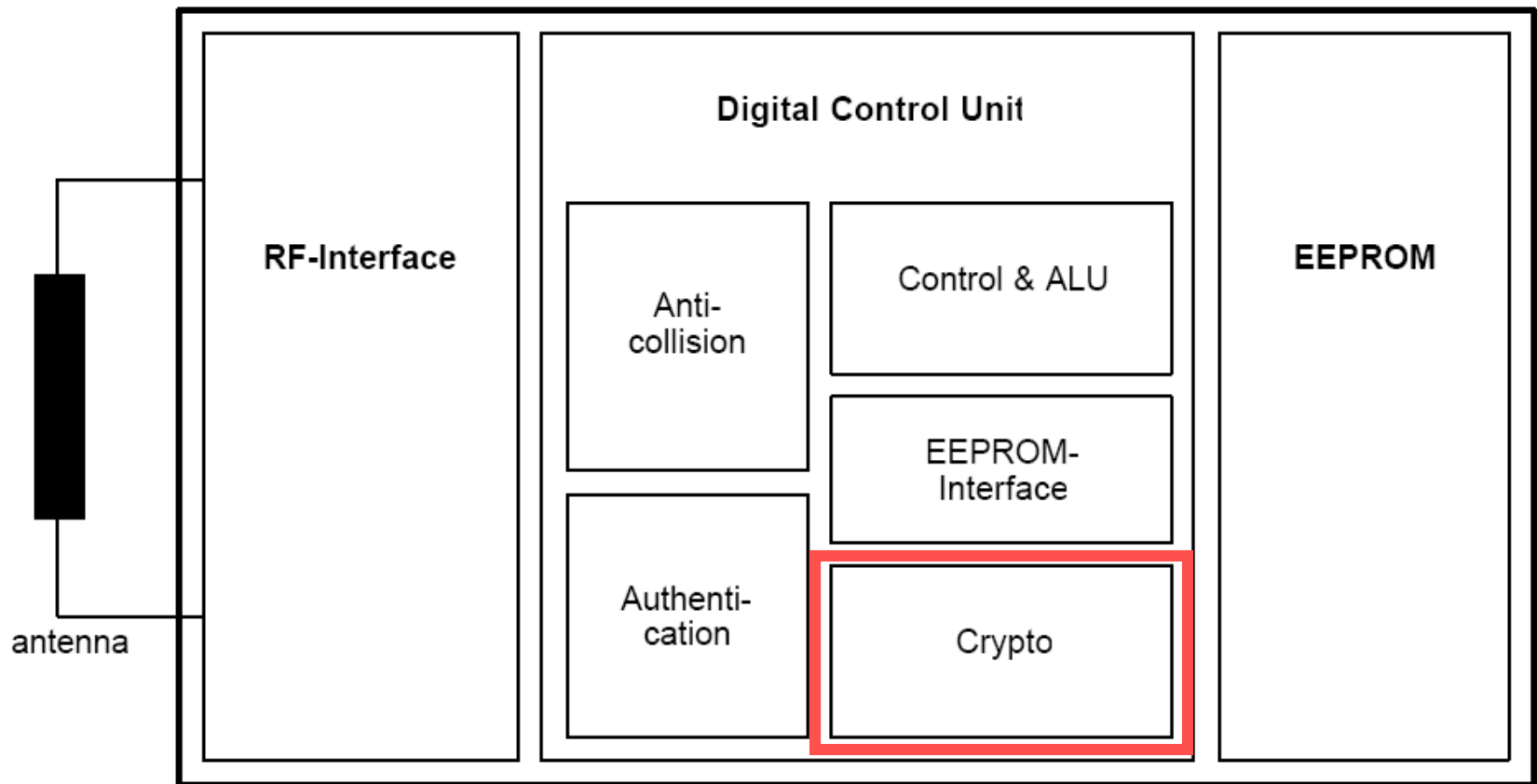


Control & Arithmetic Logic Unit

- Used for value operation
- Increment operation
- Decrement operation

Mifare Card MF1 IC S50 Architecture:

Crypto Unit



Crypto Unit

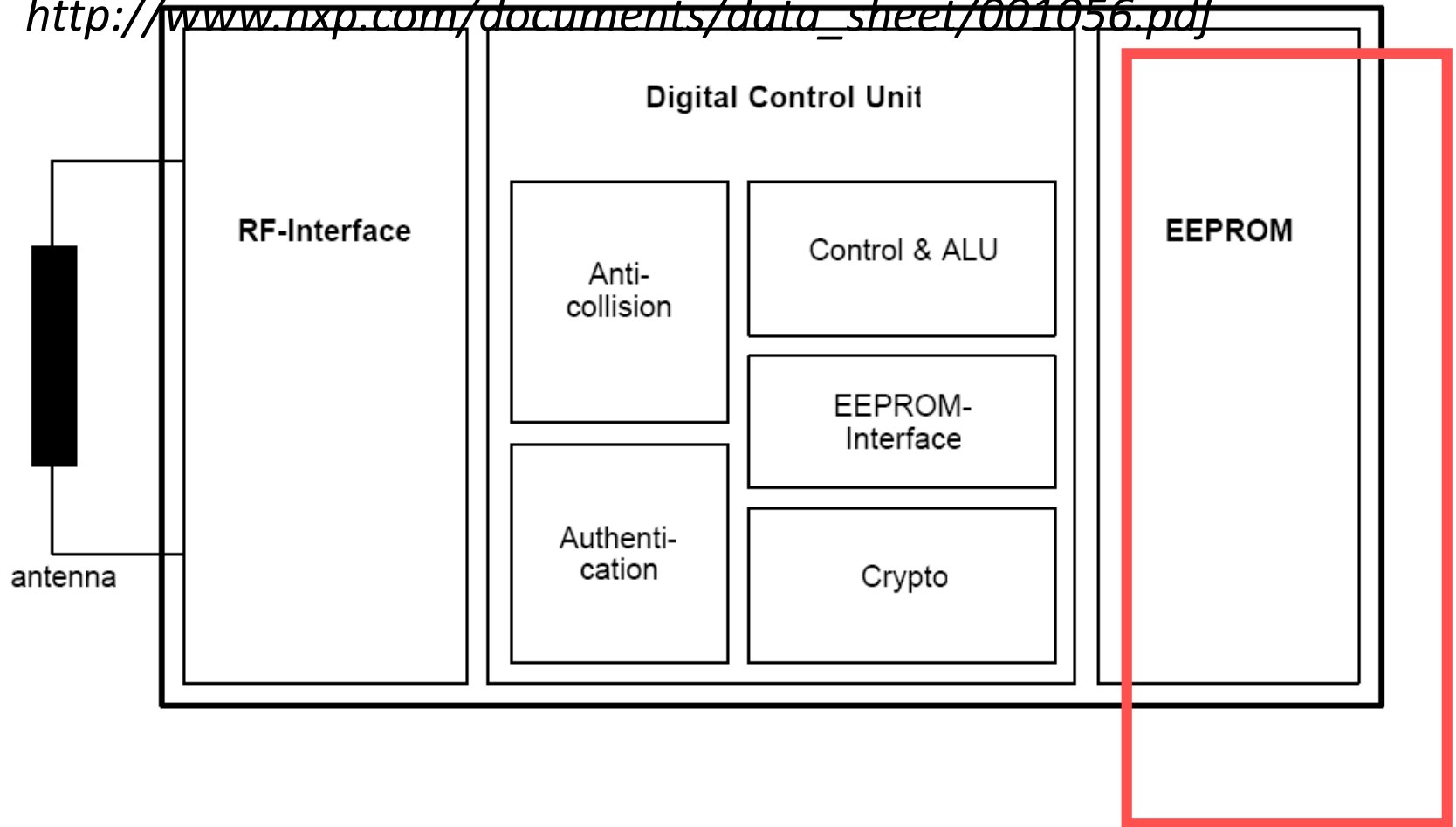
- Provides secure data exchange between the Reader and the card
- Proprietary stream cipher

Mifare Card MF1 IC S50 Architecture:

EEPROM

- Specification can be found at

http://www.nxp.com/documents/data_sheet/001056.pdf



EEPROM

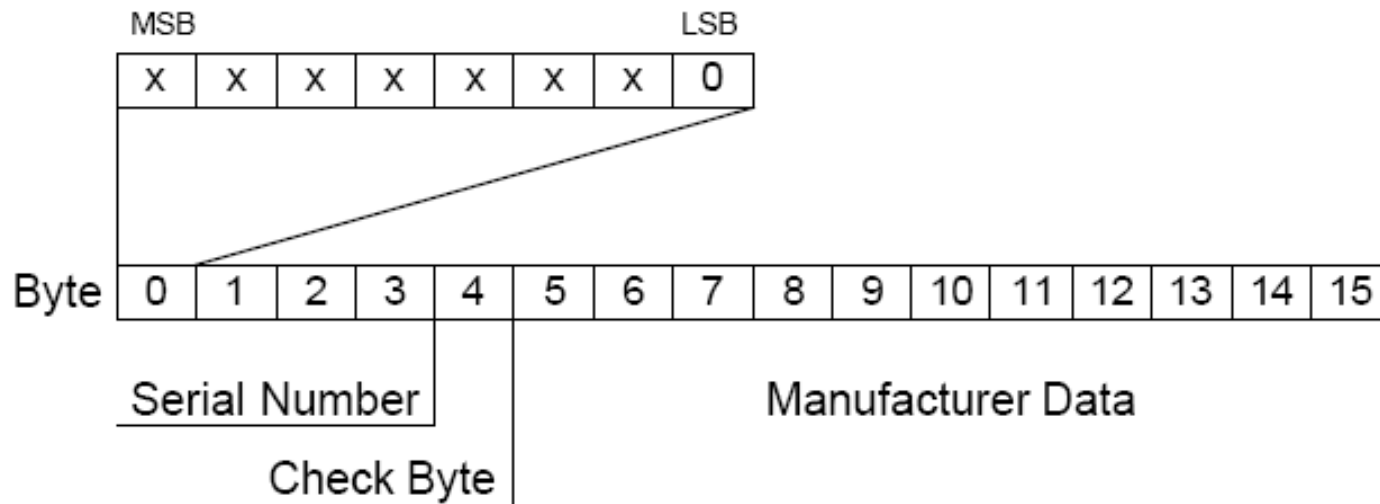
- 1K byte data storage
 - Other products might have storage up to 8K
- Organized in 16 sectors with 4 blocks each
- A block contains 16 bytes
- The last block of each sector is called “Trailer”, which contains two secret keys and programmable access conditions for the sector

Memory Organization

Sector	Block	Byte Number within a Block																Description
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
15	3	Key A					Access Bits				Key B						Sector Trailer 15	
	2																	Data
	1																	Data
	0																	Data
14	3	Key A					Access Bits				Key B						Sector Trailer 14	
	2																	Data
	1																	Data
	0																	Data
:	:																	
:	:																	
:	:																	
1	3	Key A					Access Bits				Key B						Sector Trailer 1	
	2																	Data
	1																	Data
	0																	Data
0	3	Key A					Access Bits				Key B						Sector Trailer 0	
	2																	Data
	1																	Data
	0																	Manufacturer Block

Manufacturer Block

- The first data block (block 0) of the first sector (sector 0).
- It contains the IC manufacturer data.
- Write protected (read only)



Data Blocks & Value Blocks

- Block 0 to Block 2 of all sectors can be used as data blocks (Except block 0 of Sector 0)
- Have a fixed data format

Byte Number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Description	Value			Value				Value				Adr	Adr	Adr	Adr	Adr

Sector Trailer (Block 3)

- Consists of
 - 6 bytes Key A
 - 4 bytes access condition
 - 6 bytes Key B (optional)

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)					

Access Bits

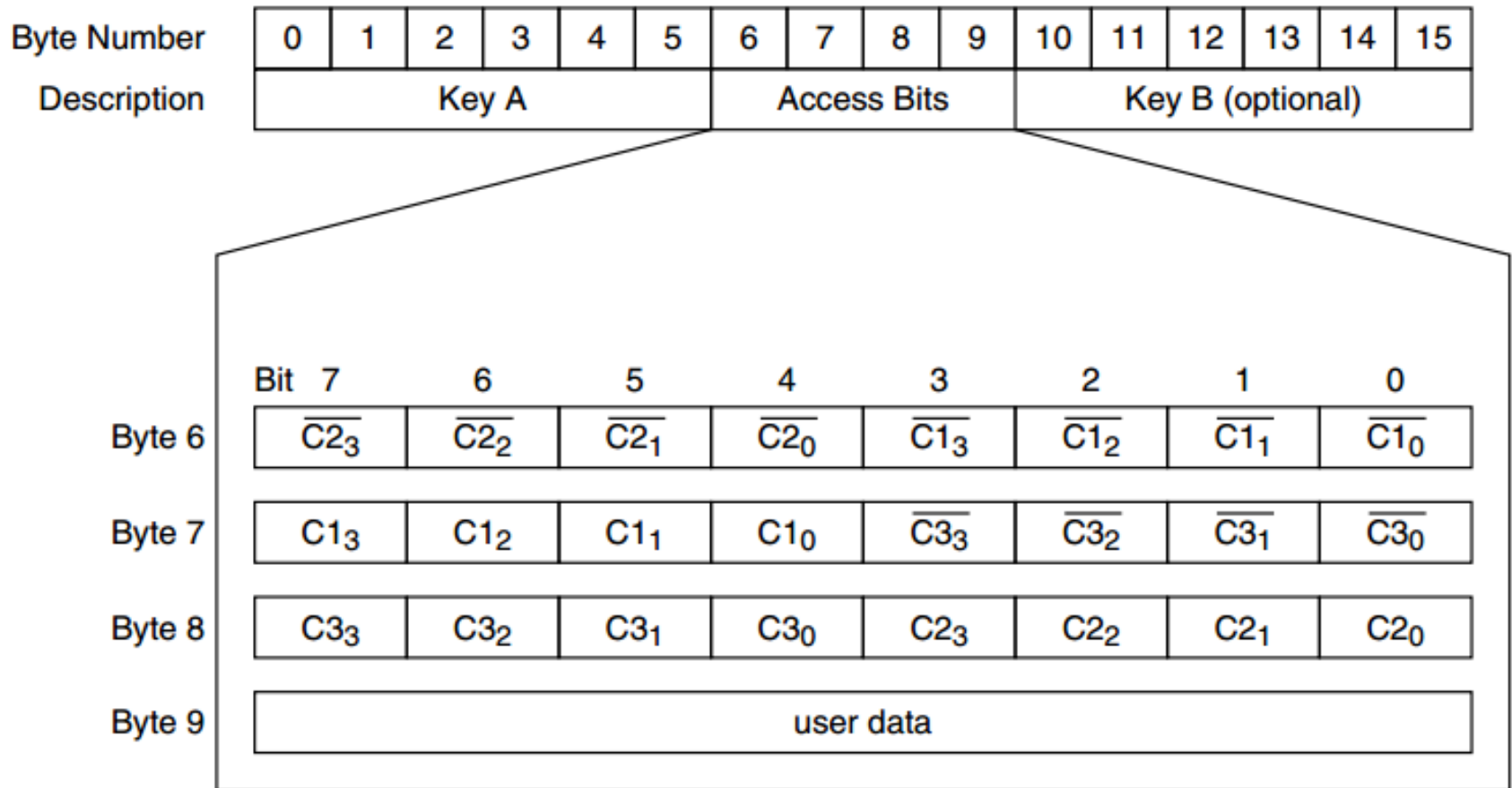
- The access conditions for every data block and sector trailer are defined by 3 bits, which are stored non-inverted and inverted in the sector trailer of the specified sector
 - 3 bits x (3 data blocks + 1 trailer) = 12 bits
 - + their complement values → 24 bits are needed

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

Operations

Operation	Description	Valid for 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 data register	value
Decrement	decrements the contents of a block and stores the result in the internal data register	value
Transfer	writes the contents of the internal data register to a block	value
Restore	reads the contents of a block into the internal data register	value

Access Bits



Access Conditions for Trailer Sector

Access bits			Access condition for						Remark
			KEYA		Access bits		KEYB		
C1	C2	C3	read	write	read	write	read	write	
0	0	0	never	key A	key A	never	key A	key A	Key B may be read
0	1	0	never	never	key A	never	key A	never	Key B may be read
1	0	0	never	key B	key A B	never	never	key B	
1	1	0	never	never	key A B	never	never	never	
0	0	1	never	key A	key A	key A	key A	key A	Key B may be read, transport configuration
0	1	1	never	key B	key A B	key B	never	key B	
1	0	1	never	never	key A B	key B	never	never	
1	1	1	never	never	key A B	never	never	never	

Access Conditions for Data Blocks

Access bits			Access condition for				Application
C1	C2	C3	read	write	increment	decrement, transfer, restore	
0	0	0	key A B ¹	key A B ¹	key A B ¹	key A B ¹	transport configuration
0	1	0	key A B ¹	never	never	never	read/write block
1	0	0	key A B ¹	key B ¹	never	never	read/write block
1	1	0	key A B ¹	key B ¹	key B ¹	key A B ¹	value block
0	0	1	key A B ¹	never	never	key A B ¹	value block
0	1	1	key B ¹	key B ¹	never	never	read/write block
1	0	1	key B ¹	never	never	never	read/write block
1	1	1	never	never	never	never	read/write block

[1] If the reader tries to authenticate any block of a sector with key B using grey marked access conditions, the card will refuse any subsequent memory access after authentication.

Example:

- Read block 3 data with response

000000000000FF078069FFFFFFFFFFFF

- Key A = 000000000000

- Key B = FFFFFFFFFFFFFF

- Access Bits = FF 07 80

Example:

- ▶ Byte 6 = FF

$$\overline{C2_3 C2_2 C2_1 C2_0 C1_3 C1_2 C1_1 C1_0} = FF = 11111111$$

$$\rightarrow C2_3 C2_2 C2_1 C2_0 C1_3 C1_2 C1_1 C1_0 = 00000000$$

- ▶ Byte 7 = 07

$$C1_3 C1_2 C1_1 C1_0 \overline{C3_3 C3_2 C3_1 C3_0} = 07 = 0000001111$$

$$\rightarrow C1_3 C1_2 C1_1 C1_0 C3_3 C3_2 C3_1 C3_0 = 00001000$$

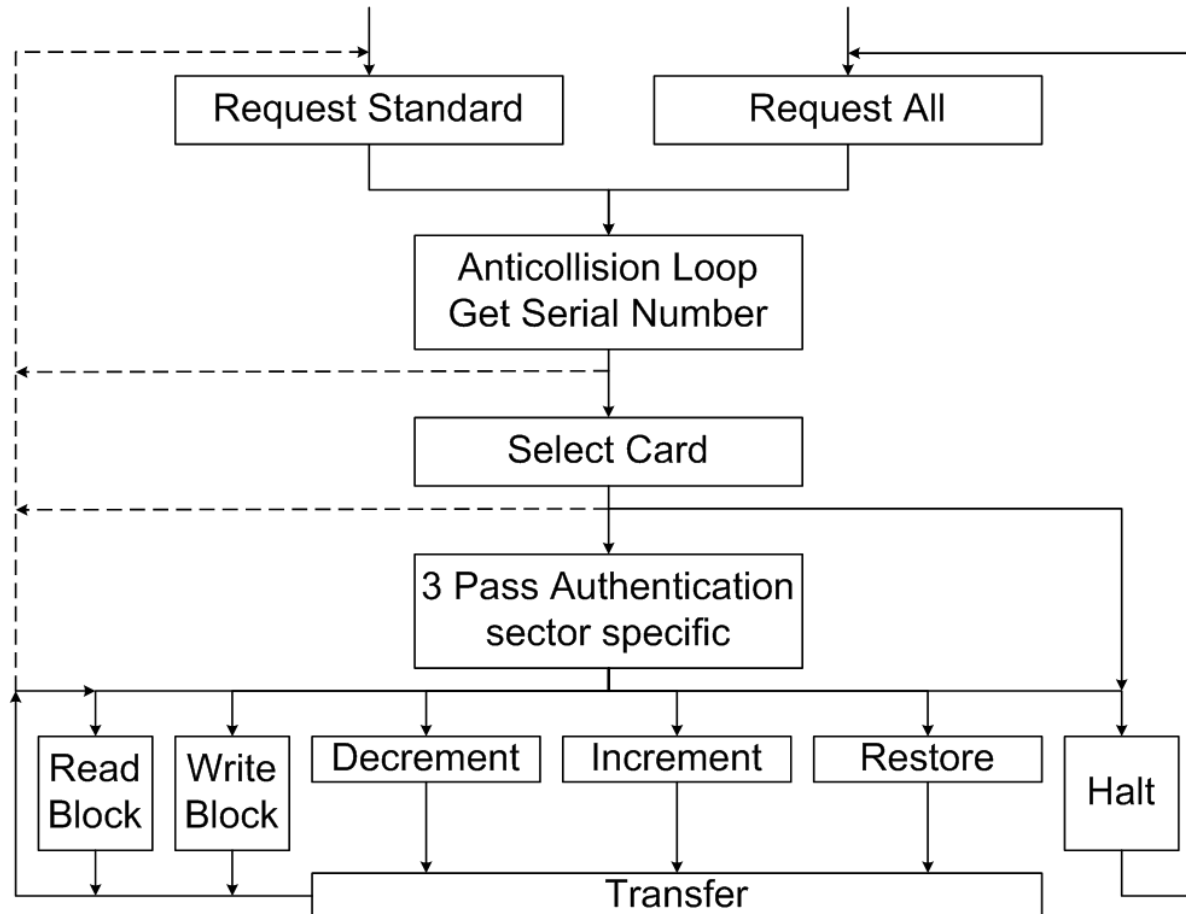
- ▶ Byte 8 = 80

$$C3_3 C3_2 C3_1 C3_0 C2_3 C2_2 C2_1 C2_0 = 80 = 10000000$$

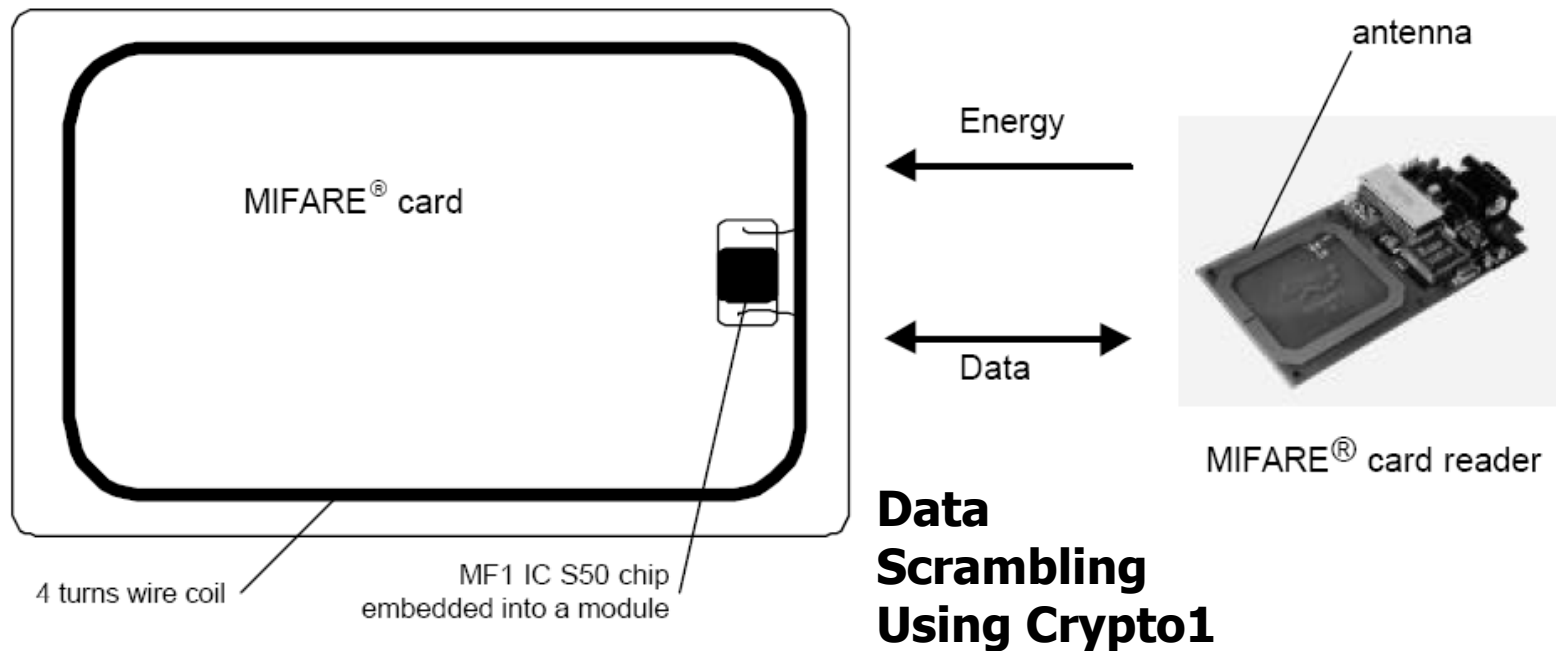
Access Conditions

Block No.	Access Bits			Conditions
	C1	C2	C3	
0	0	0	0	Data: read/write/increment/decrement/transfer/restore accessed by Keys A B
1	0	0	0	Data: read/write/increment/decrement/transfer/restore accessed by Keys A B
2	0	0	0	Data: read/write/increment/decrement/transfer/restore accessed by Keys A B
3	0	0	1	Keys: Key A can “Write Key A / Read or Write Key B/ Read/Write access bits”

Transaction Sequences



Communication Mechanism



RF Data Scrambling

- Data is scramble using Crypto1 Cipher architecture
- The architecture is composed of linear and non-linear Feedback Shift Registers with mapping functions f_a , f_b , and f_c
- RF Data Exchange is encrypted by the “out” stream cipher
- **NOTE:** Crypto 1 has been broken!
 - Switch Mifare Classic to other products, e.g. Mifare Plus

Possible Attacks on Smart Card

- *duplication*: illegal copying of card content from one to another
- *UV or X-ray inspection*: use high efficiency UV or X-ray to inspect the memory areas to extract important information like PIN, secret key and public key
- *EM analysis*: use electron microscope to inspect the internal structure of the mask
- *confusion*: disturb the power supply/frequency during PIN verification to confuse the accurate enter of PIN and allow access to the protected memory

General Smart Card Security Features

- *Against UV or X-ray inspection:*
 - Using implementation to avoid visible of ROM Code
- *Against EM analysis:*
 - Address Scrambling of memories
- *Against duplication:*
 - Security PROM Hardware Protected
 - Unique Chip Identification Number
 - Move Code Blocking
- *Against Differential Power Analysis*
 - Random Wait State (Advance)
 - Current Scrambling Generator (Advance)

Is Smart Card Secure?

- There is no 100% secure/perfect system available
- System design and built for minimal attack risk can be treated as secure
- Secure system are evaluated/classified in different levels using international standards such as Common Criteria

Your Mission



- Understand Smart-card Security
- Complete the lab exercise and assignment

