Advanced Card Systems Ltd.
Card & Reader Technologies

Memory Card Overview

CARD & READER TECHNOLOGIES

Contents

- SLE 4442
- SLE 4428
- SLE 4436
- MiFare Series
    - Ultralight
    - MiFare Classic
    - MiFare Plus

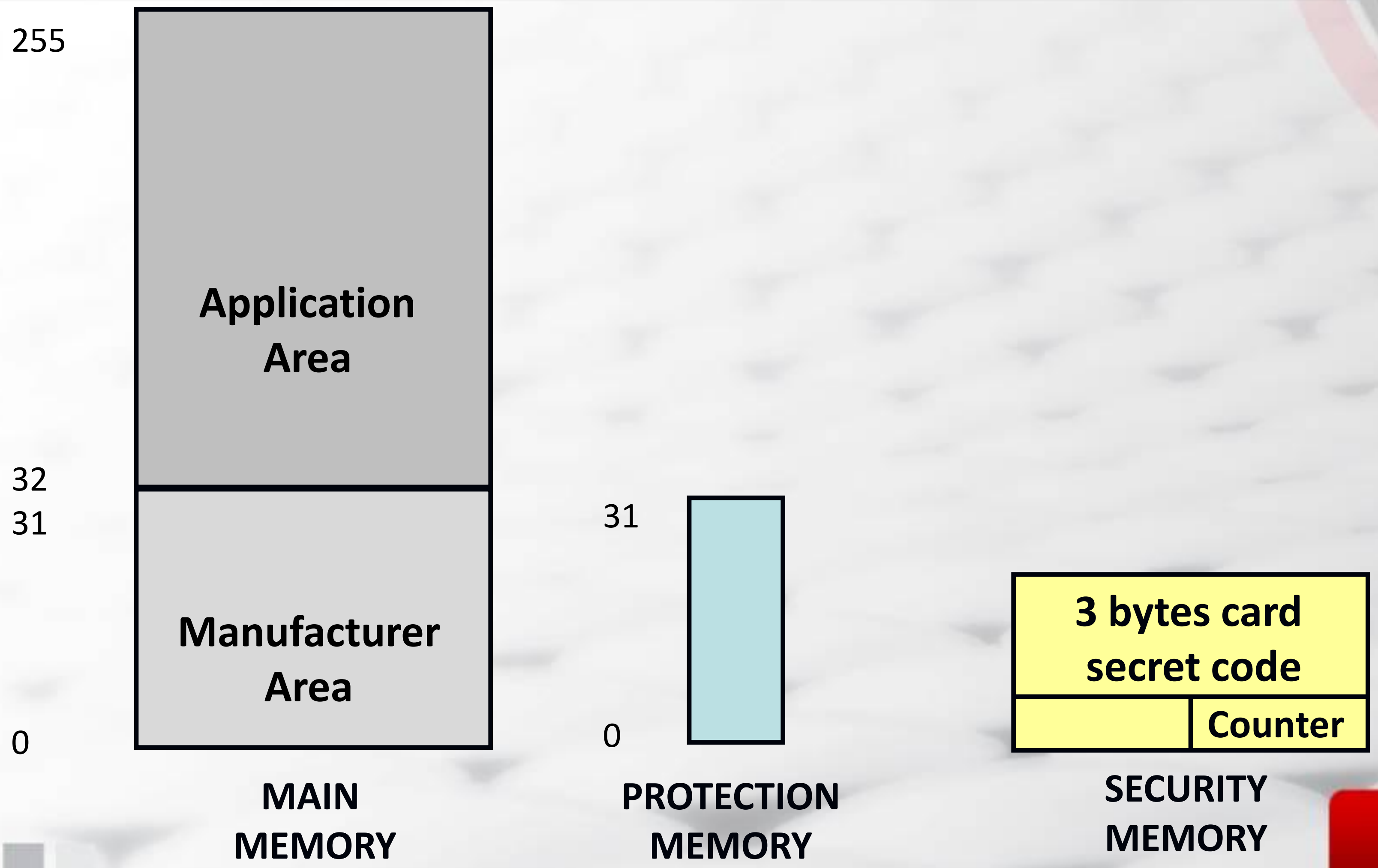
SLE4442

CARD & READER TECHNOLOGIES

Main Features

- 256 x 8 bits of application EEPROM
- 3 bytes of card secret code
- 3 bits of error counter
- 32 bits of memory protection control
- 5 volts (10 mA)
- 6 contacts
- Erase (virgin) state of 1

Memory Structure



255

Application Area

32

31

Manufacturer Area

0

MAIN MEMORY

31

0

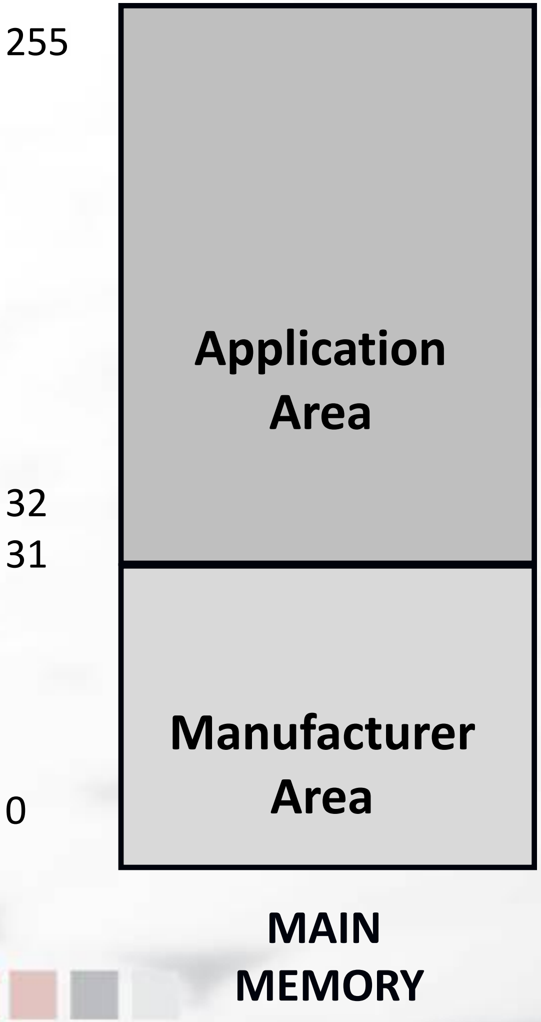
PROTECTION MEMORY

3 bytes card secret code

Counter

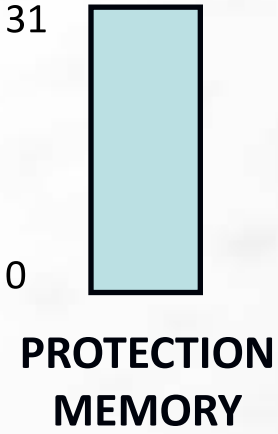
SECURITY MEMORY

Main Memory



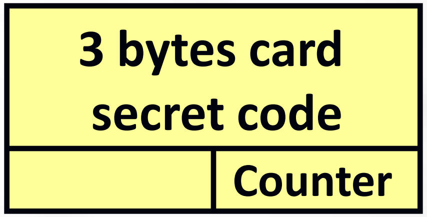
- Chip manufacturer reference
- Chip type and version
- Card manufacturer reference
- Card serial number
- Manufacturer Area is byte-wise write/erase lockable by the Protection Memory
- Application Area can be written onto/erased after presentation of the CSC
- Main Memory is entirely free read

Protection Memory



- 32 x 1 EEPROM bits used to protect 32 bytes of Manufacturer Area
- Free read Protection Memory
- Setting a bit write/erase locks the corresponding byte in the Manufacturer Area
- Protection bit can only be set by sending the address and the data to be protected
- A matched content sets the protection bit

Security Memory



SECURITY MEMORY

- ❑ 4 bytes of EEPROM comprising 3 bytes CSC and 3 bits of error counter
- ❑ Free read error counter
- ❑ CSC requires correct presentation to be read (000000)
- ❑ Wrong CSC presentation results in setting a bit in the counter to 0
- ❑ Correct CSC presentation is required to update the CSC

SLE-4442: Reader Emulation Commands

- ❑ The memory card does not comply with ISO-7816 Part 3, and therefore does not have ISO commands.
- ❑ To simplify application development and upgrade, it is better for the reader to perform an emulation command that will make the card look like a CPU card.

Card Primitive Signaling

- Reset
- Command Mode (7 commands)
  - Read; update main memory
  - Read; write protection memory
  - Read; update security memory
  - Compare verification data
- Outgoing Data Mode
- Processing Mode

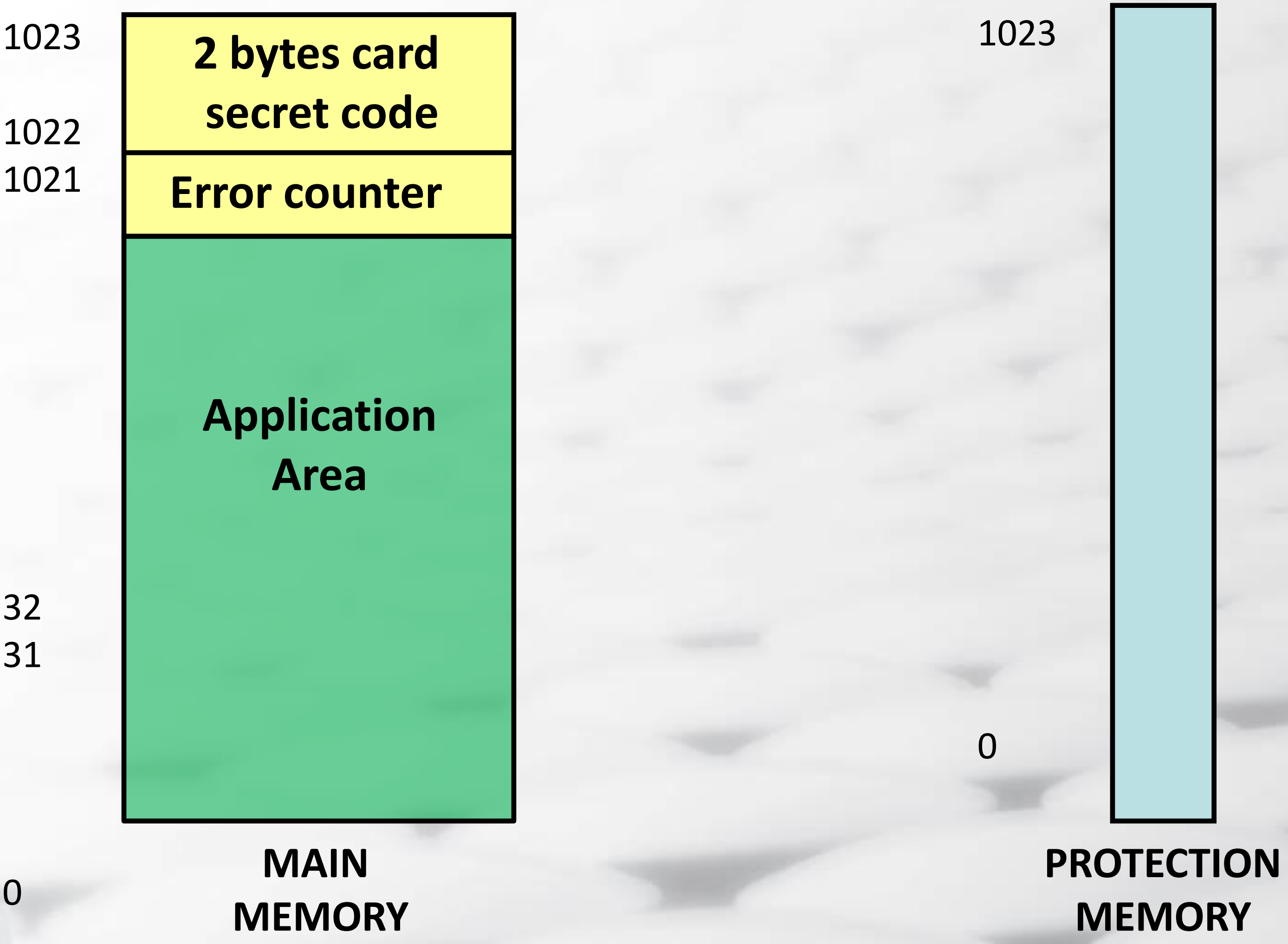
SLE4428

CARD & READER TECHNOLOGIES

Main Features

- 1024 x 8 bits of EEPROM
- 2 bytes of card secret code (03FE-03FF)
- 8 bits of error counter (03FD)
- 1024 bits of memory protection control
- 5 volts
- 6 contacts
- Erase (virgin) state of 1

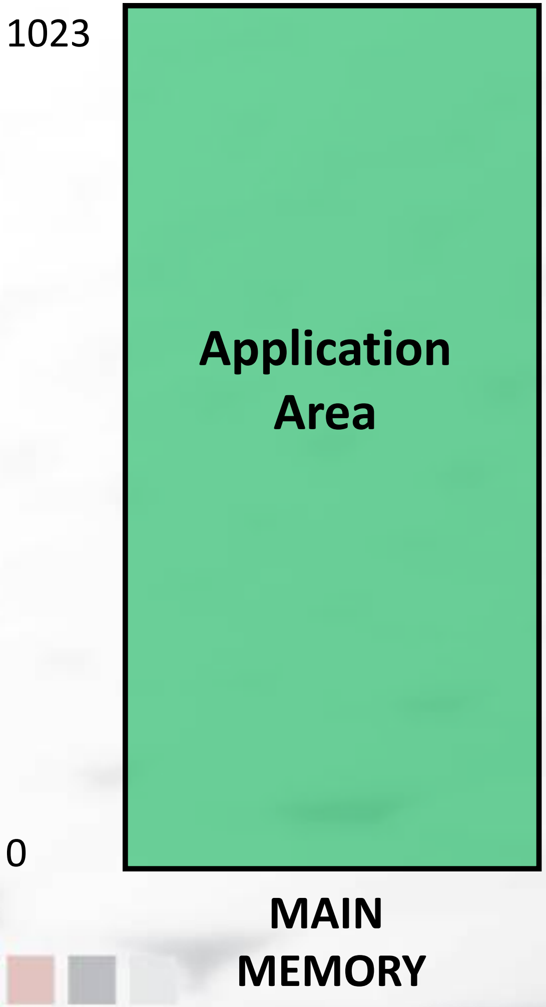
Memory Structure



1023
2 bytes card secret code
1022
1021
Error counter
Application Area
32
31
0
MAIN MEMORY

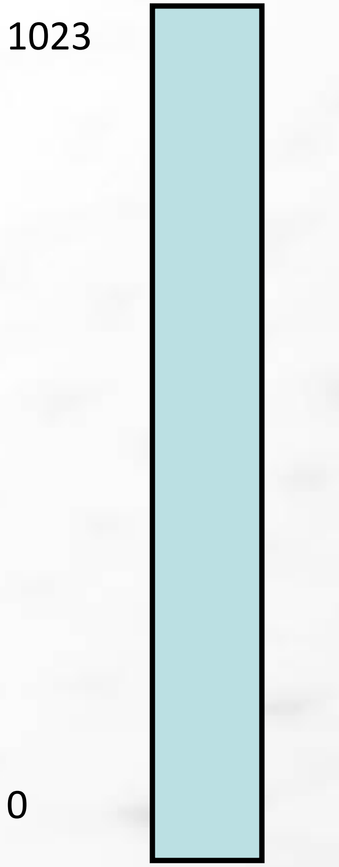
1023
0
PROTECTION MEMORY

Main Memory



- □ Manufacturer Area is byte-wise write/erase lockable by the Protection Memory
- □ Application area can be written onto/erased after presentation of the CSC
- □ Memory 0 to 1021 is always free read
- □ CSC is always 0000 before presentation/wrong presentation
- □ Main memory is entirely free read after correct CSC presentation

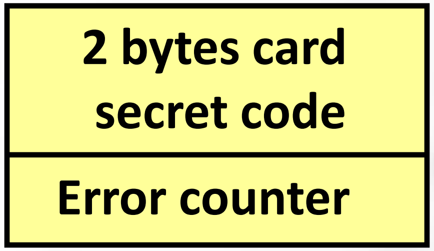
Protection Memory



PROTECTION MEMORY

- 1024 x 1 EPROM bits used to protect the 1024 bytes manufacturer area
- Protection memory is free read
- Setting a bit write / erase lock the corresponding byte in the main memory
- Protection bit can only be set by sending the address and the data to be protected
- A matched content sets the protection bit

Security Memory



2 bytes card secret code

Error counter

SECURITY MEMORY

- 3 bytes of EEPROM comprising 2 bytes of CSC and 8 bits of error counter
- Free read error counter
- CSC cannot be read (000000) before correct presentation
- Wrong CSC presentation will result to a bit in the counter being set to 0
- Correct CSC presentation is required to update the CSC

SLE-4428: Reader Emulation Commands

- The memory card does not comply with ISO-7816 part 3, and therefore does not have ISO commands.
- To ease application development and upgrade, it is better for the reader to perform an emulation command that will make the card look like a CPU card.

Card Primitive Signaling

- Reset
- Command Mode (7 commands)
  - Read with Address Increment
  - Write / Erase
  - CSC Verification

SLE4436

CARD & READER TECHNOLOGIES

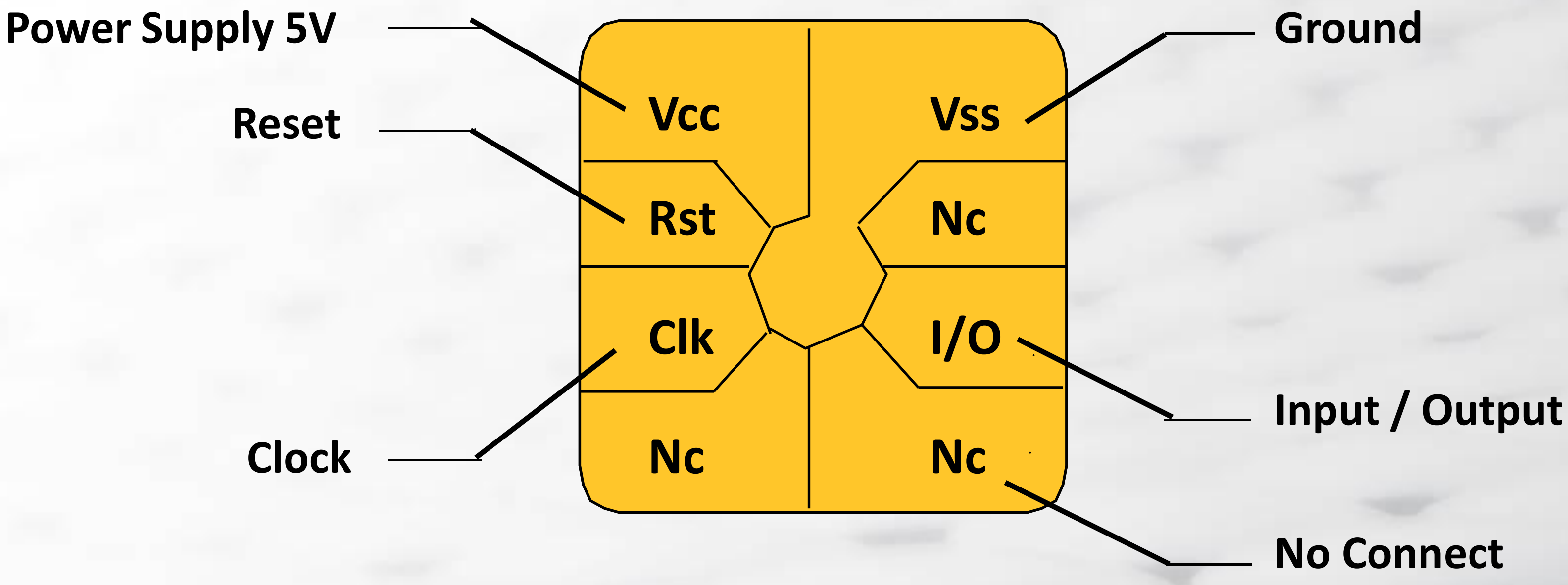
SLE-4436: Second Generation Telephone Card

- ❑ 4436 Specifications
- ❑ Memory Organization
- ❑ Card Life Phases
- ❑ Security Features
- ❑ Card Commands

4436 Specifications

- Memory divided into different areas:
  - 24 bits Manufacturer Area
  - 40 bits Issuer Area
  - 40 bits Abacus Counter Area
  - 16 bits Data Area 1 (eg. certificate)
  - 48 bits Authentication Key Area
  - 64 bits Data Area 2 or 48 bits Authentication Key Area
- Count up to 21 064 tokens (not reloadable)
- Pull out protection
- Active card authentication

Pin Assignments

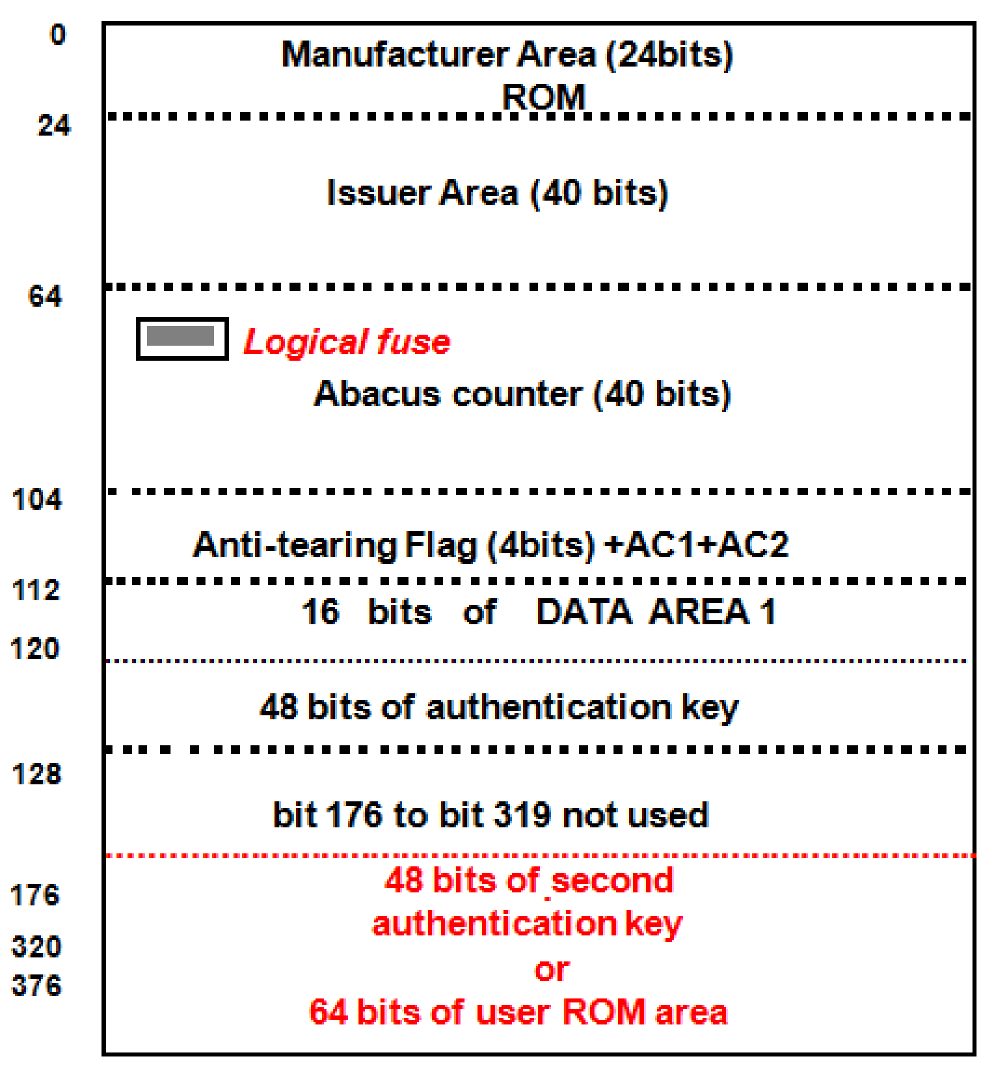


ISO 7816 – 1,2 Compatible

Electrical Characteristics

- ❑ 5V voltage supply (VCC)
- ❑ Low power consumption, < 5mA
- ❑ Compatible with SLE – 4406
- ❑ Operating range: -35°C to +80°C
- ❑ Ten years minimum data retention
- ❑ 100K erase write cycle
- ❑ 5 min. EEPROM programming time

Memory Organization



0
Manufacturer Area (24bits)
ROM

24
Issuer Area (40 bits)

64
Logical fuse
Abacus counter (40 bits)

104
Anti-tearing Flag (4bits) +AC1+AC2

112
16 bits of DATA AREA 1

120
48 bits of authentication key

128
bit 176 to bit 319 not used

176
320
376
48 bits of second authentication key
or
64 bits of user ROM area

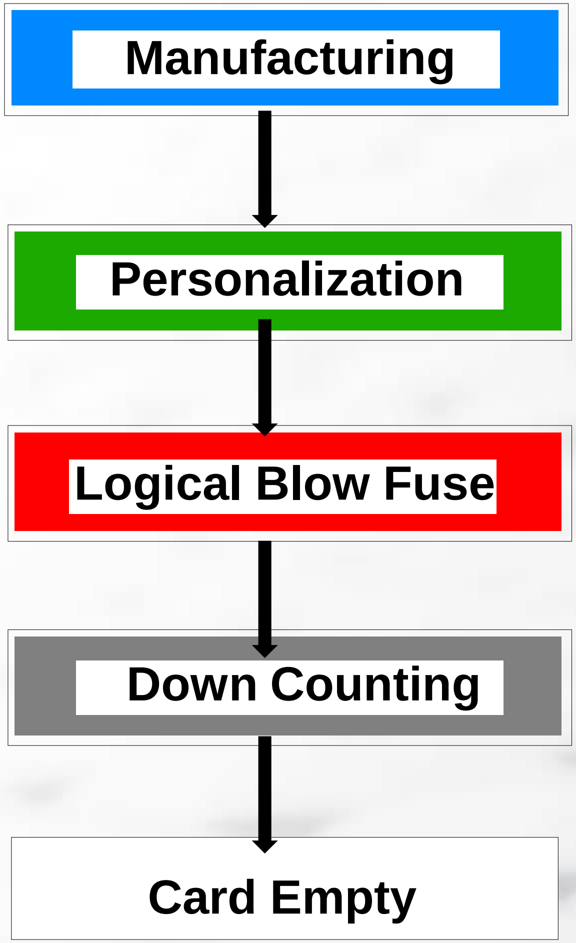
Additional Features: Comparison to SLE-4406

- Card cryptographic authentication algorithm
- More memory
  - 80 bit extended Issuer area with a 48 bit authentication key
  - 16 bit extended issuer area with two 48 bit authentication keys
- Protection of the counter content against power down (pulling the card out)

Purpose of Additional Features

- Authentication Algorithm
  - To authenticate the card by the terminal
  - To avoid fabrication or counterfeiting of the card
- Anti Pull-out Protection
  - To avoid any loss of units if power goes down during an operation
- User Memory
  - To be able to store Issuer or User data after card personalization

Card Life Phases



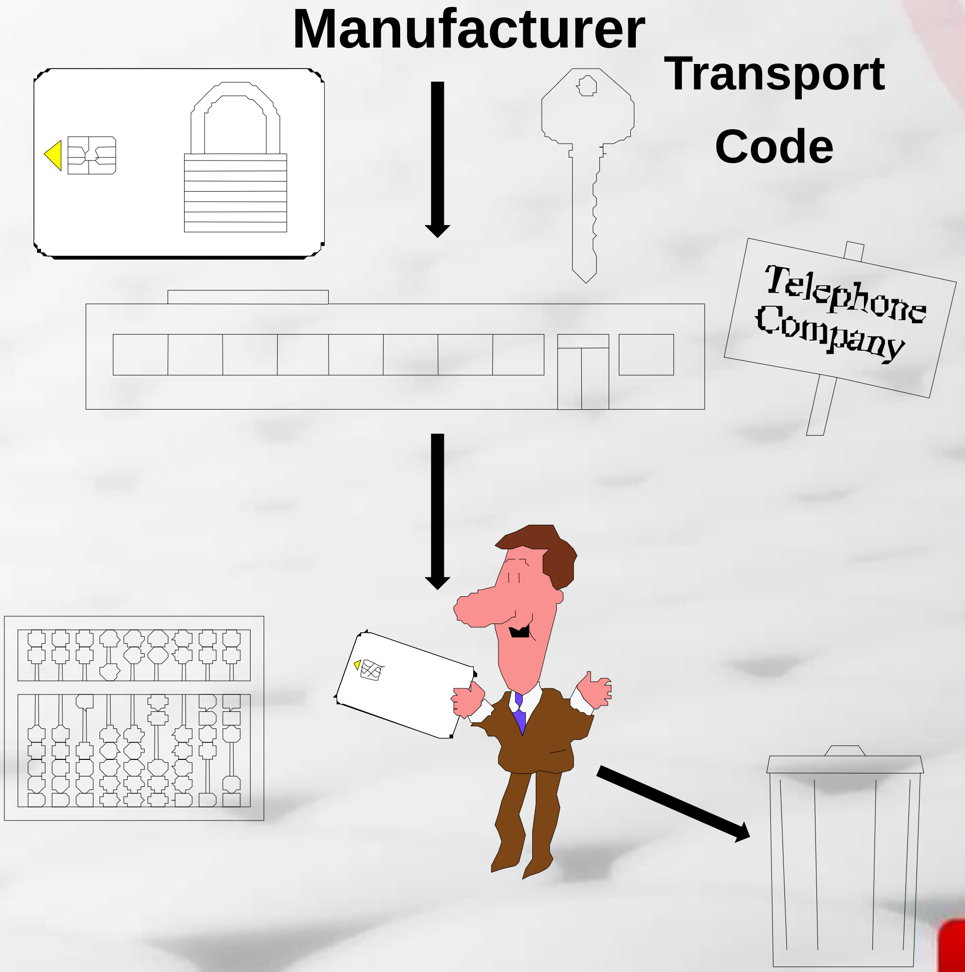
Manufacturing

Personalization

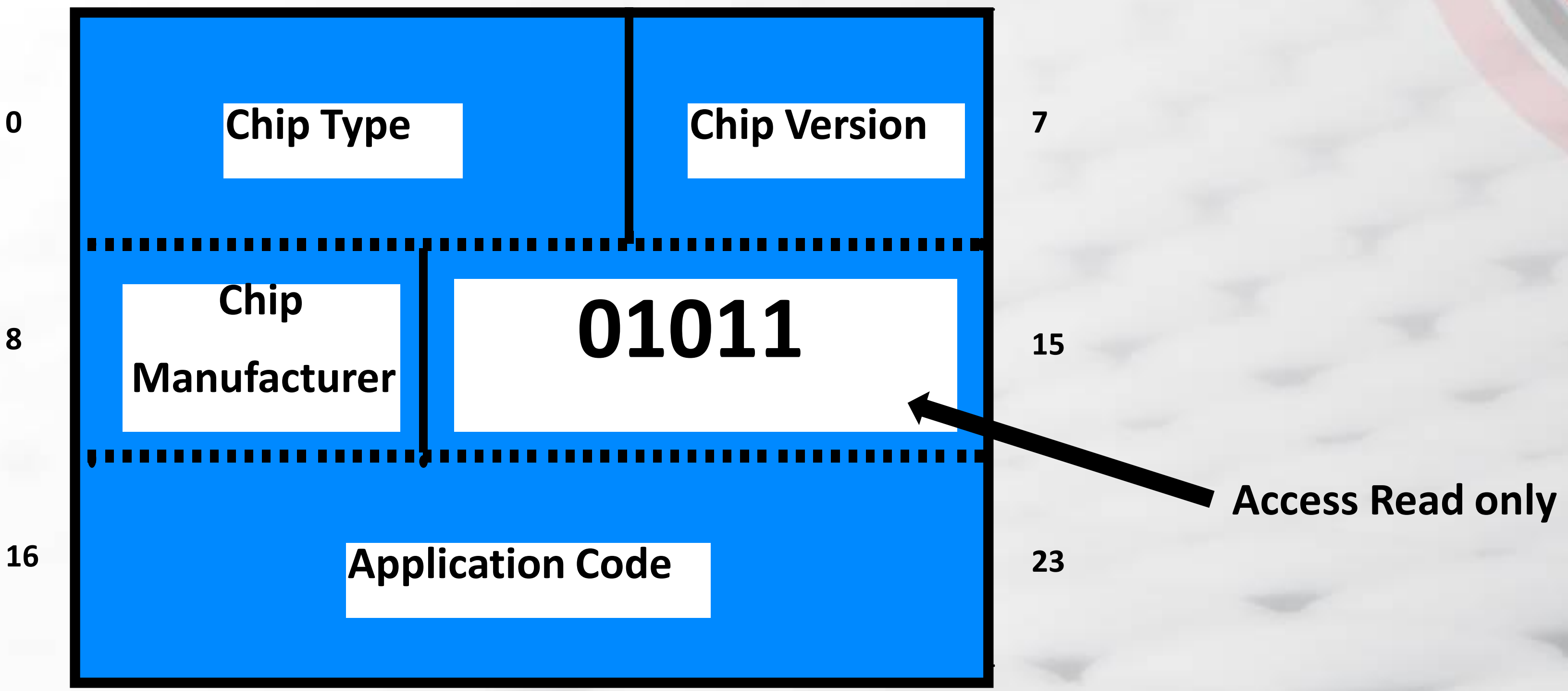
Logical Blow Fuse

Down Counting

Card Empty



Manufacturer Area



0

Chip Type

Chip Version

7

8

Chip Manufacturer

01011

15

Access Read only

16

Application Code

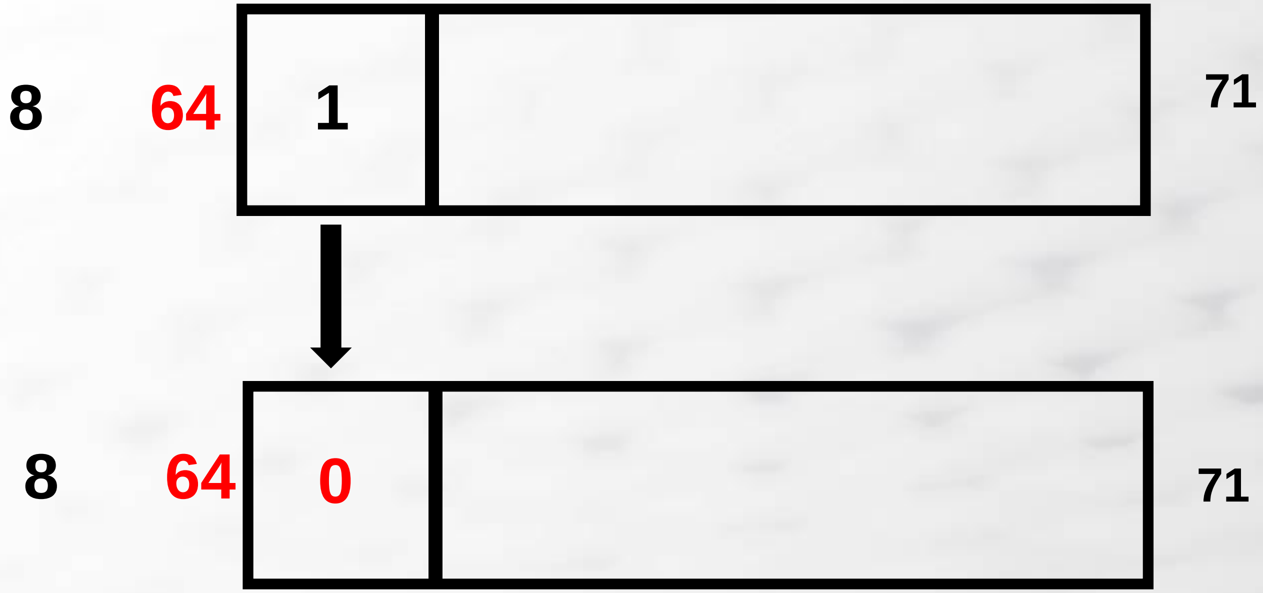
23

The exact contents of the manufacturer area will be communicated when ordering is placed.

Personalization

- ❑ Present Transport Code
- ❑ Write Issuer Area
- ❑ Clear Counters
- ❑ Blow Logical Fuse
- ❑ Set Initial Value

Fuse Blow



Writing to the Logical Fuse *(Bit 64) changes the 4406 from Personalization Mode to Count Down Mode.*

This is irreversible.

Before and After Fuse Blow

Before

(Personalization Mode)

- 24-bit Manufacturing information (read only)
- Protected by transport code
- 7 attempts of presenting the transport code before the card becomes useless
- Loadable counter with value of 0-33,352

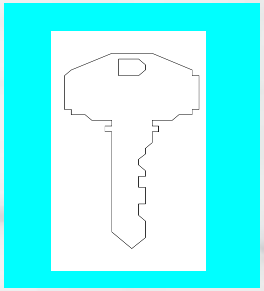
After

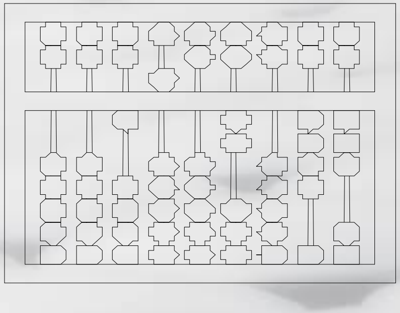
(Countdown Mode)

- Down Counter from loaded value to zero
- Issuer and manufacturer information is read only
- No access to key area after the fuse is blown
- Extended data area READ / WRITE (not erase)

Count Down Phase

- Verify Issuer Data and Manufacturer Data for valid card
- Count down units with Authentication, Issue Service
- If empty, throw away





Transport Code Presented

	W	E	R
Manufacturer Area (24 bits)	N	N	Y
Issuer Area (40 bits)	Y	N	Y
Transport Code	Y	Y*	Y
Anti-Tearing Flags (4 bits)	Y*	Y*	Y
AC1	N	N	1
AC2	Y	N	Y
16 bits data	Y	N	Y
48 bits key	Y	N	Y
bit 176 to bit 319 not used			
48 bits 2nd key or 64 bits data	Y	N	Y

Y* = indirect

Countdown Mode

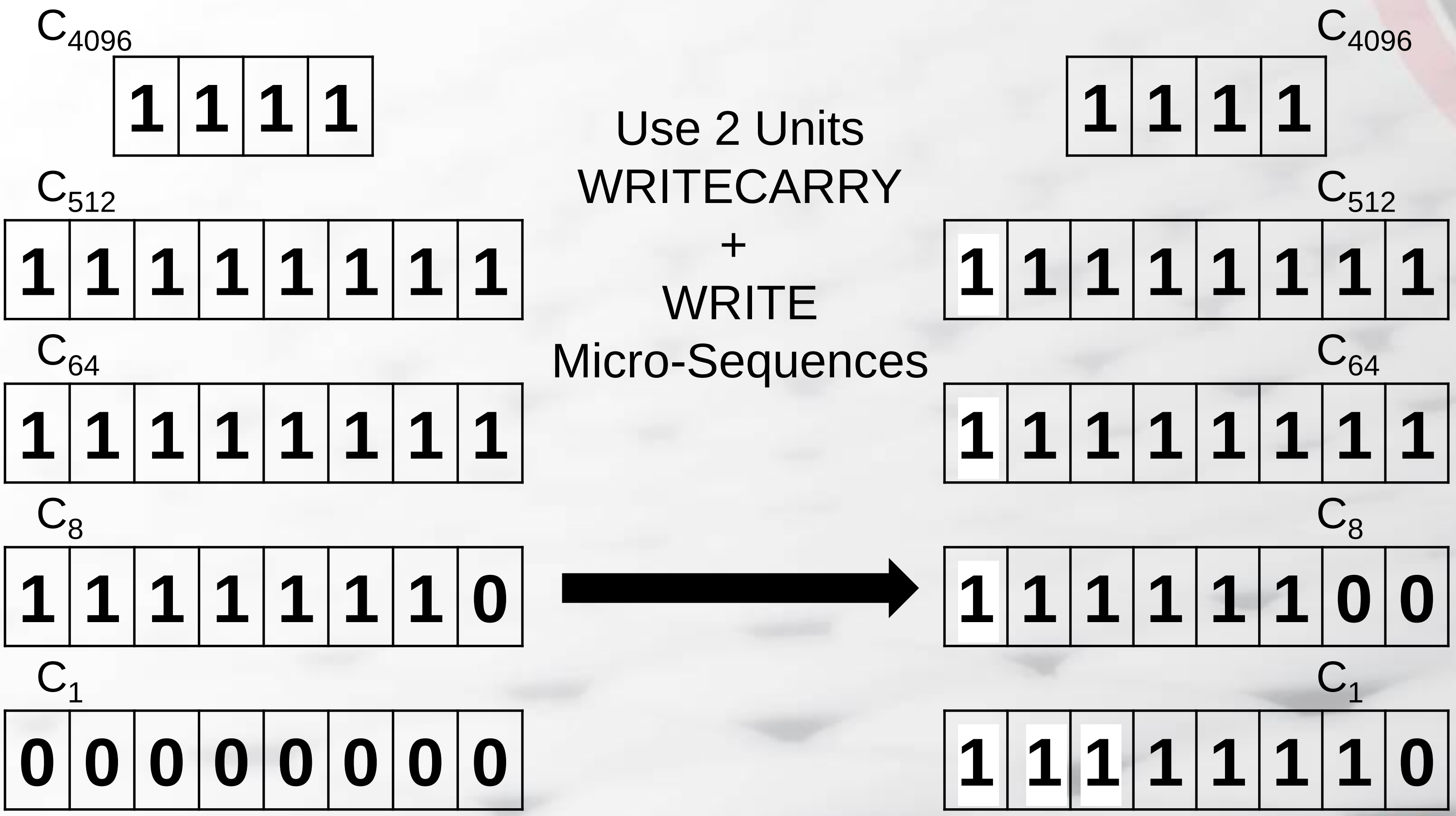
	W	E	R
Manufacturer Area (24 bits)	N	N	Y
Issuer Area (40 bits)	N	N	Y
Transport Code	Y*	Y*	Y
Anti-Tearing Flags (4 bits)	Y*	Y*	Y
AC1	N	N	1
AC2	N	N	Y
16 bits data	Y	N	Y
48 bits key	N	N	1
bit 176 to bit 319 not used			
48 bits 2nd key or 64 bits data	N Y	N OR N	1 Y

Y* = indirect

Count Mode

- Any unwritten counter bit can be written onto anytime.
- WRITE Micro-Sequence
  - The counter can be loaded with any value during personalization.
  - A new value can be assigned to the counter without affecting and resetting all intermediate values.
  - Counters C1, C8, C64 and C512 can be erased (refilled) by writing an unwritten bit onto the next level counter.
- WRITECARRY Micro-Sequence
  - Counter C4096 cannot be erased.
  - The card does not perform carry propagation between counters.
  - Carry propagation must be performed by the reader with additional WRITECARRY instructions.

Count Mode Scheme



C_{4096}	1 1 1 1	1 1 1 1
C_{512}	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1
C_{64}	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1
C_8	1 1 1 1 1 1 1 0	1 1 1 1 1 1 0 0
C_1	0 0 0 0 0 0 0 0	1 1 1 1 1 1 1 0

Use 2 Units
WRITECARRY
+
WRITE
Micro-Sequences

Counter status

Erasing Counter with WRITECARRY

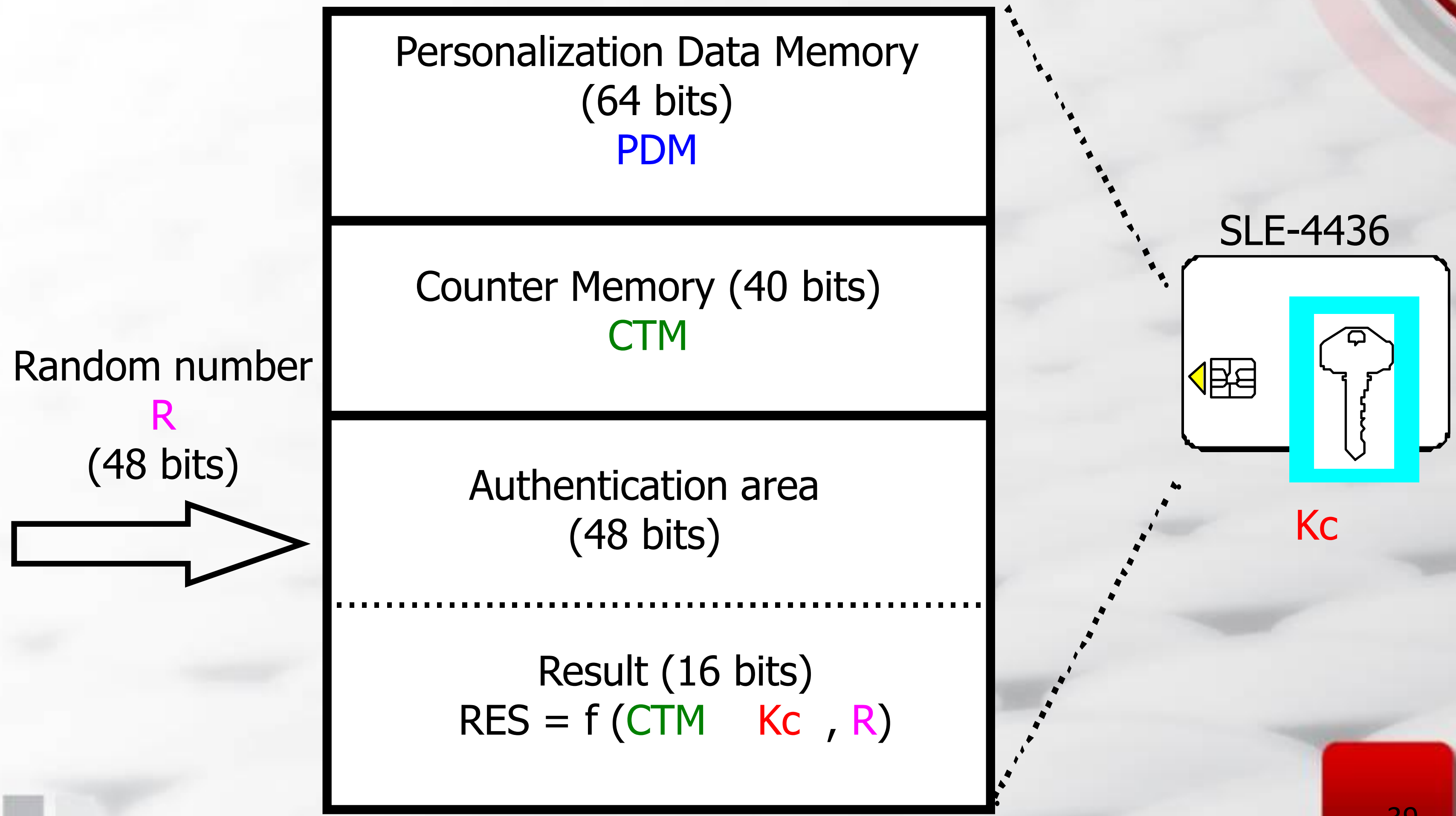
To erase counter	WRITECARRY in
C_8	C_8
C_8	C_{64}
C_{64}	C_{512}
C_{512}	C_{4096} or Logical Fuse
C_{4096}	Impossible

***The WRITECARRY micro-sequence must be performed** on an unwritten bit to erase a counter.*

Security Features

- The manufacturer area contains information unique to one application.
- The manufacturer area cannot be modified.
- Protection is provided by the Transport Code during delivery.
- Logical security features & chip layout avoid physical/electrical attack.
- It is equipped with a Cryptographic Card Authentication Algorithm.
- The SAM is integrated into each application.

Authentication Algorithm Concept



Personalization Data Memory
(64 bits)
PDM

Counter Memory (40 bits)
CTM

Random number
R
(48 bits)

Authentication area
(48 bits)

Result (16 bits)
RES = f (CTM Kc , R)

SLE-4436

Kc

Card Authentication Signaling

- Apply address reset
- Clock to the address of AC1 (110) using key 1 or AC2 (111) using key 2
- Apply dummy write signaling on AC1 or AC2
- Apply 177 clocks for loading the data stored in the chip
- Follow through with 48 clocks for the 48 bit challenge
- Start from clock 226. Every next m clock computes a response bit, m=160 for 4436
- The maximum response is 16 bits

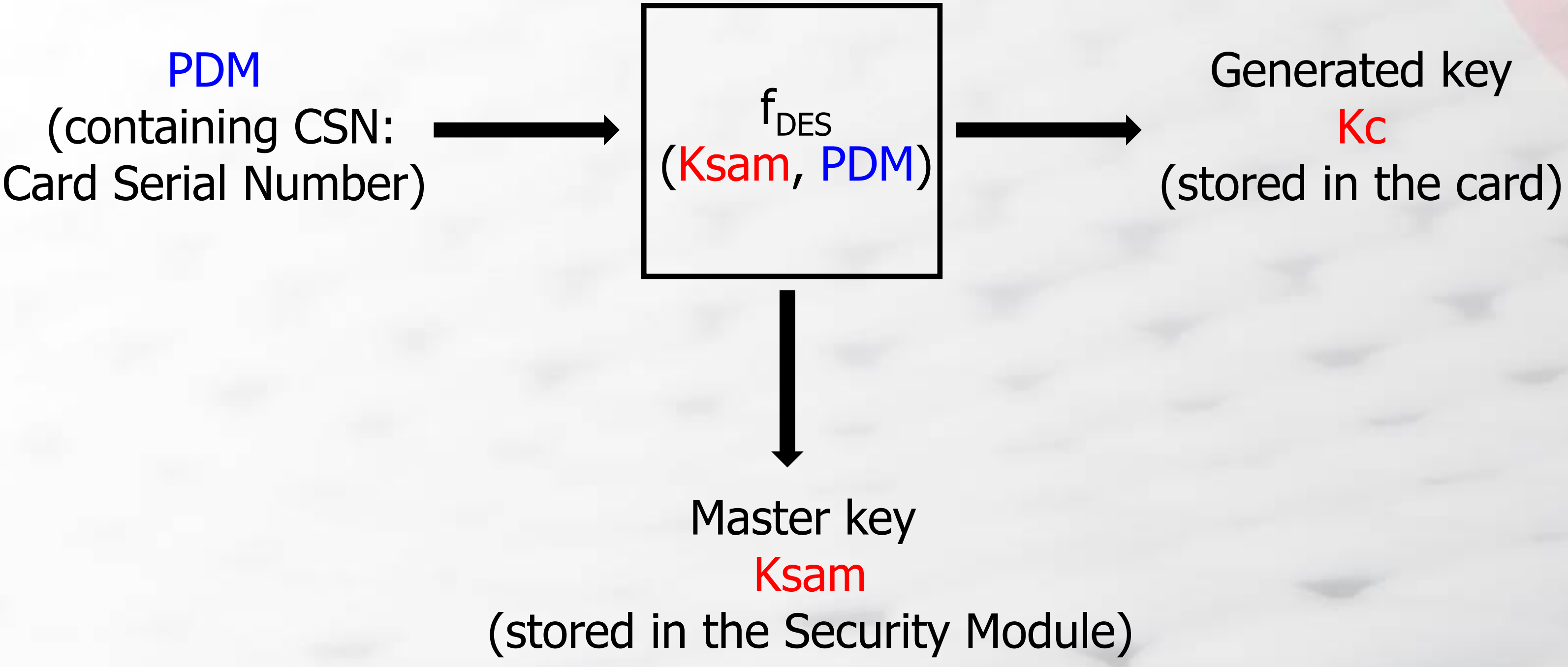
Security Access Module (SAM)

- Protection of the application key, Ksam
- Calculation of the card key, Kc = f3DES (PDM, Ksam)
- Generation of the random number, R
- Execution of the authentication algorithm
- Comparison of the calculated result with the result sent by the card
- One SAM integrated into the host with one Ksam key by the application

SAM: Characteristics

- ISO 7816-3 compliance
- Built on top of a CPU smart card
- Command set basic requirements:
  - DIVERSIFICATION of a master key in the SAM
  - GET_RAND to send a random number to the card
  - AUTHENTICATE to compare the result of the card

Key Diversification



PDM
(containing CSN:
Card Serial Number)

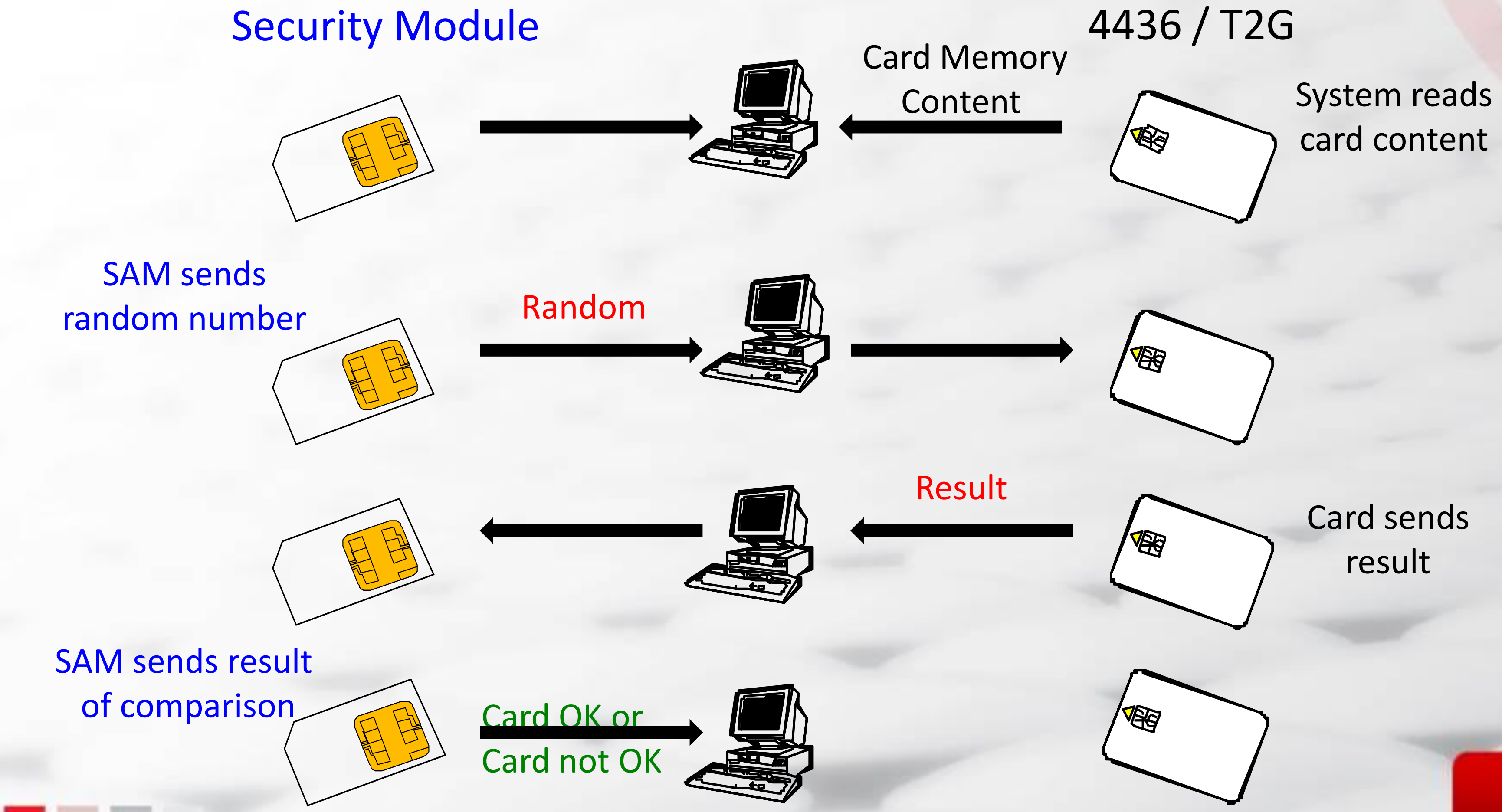
f_{DES}
(Ksam, PDM)

Generated key
Kc
(stored in the card)

Master key
Ksam
(stored in the Security Module)

Kc always depends on a variable: the CSN.

Authentication Mechanism



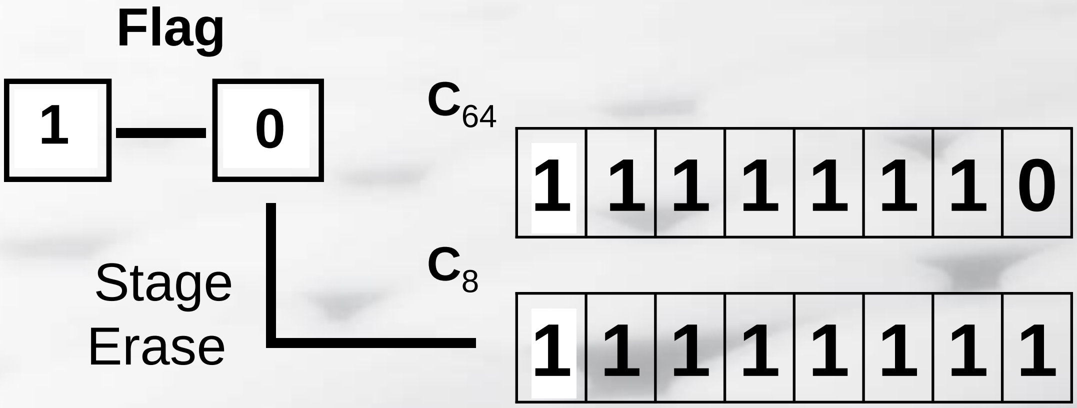
Anti Pull Out Protection Concept

- Problem:
  - Units could be lost if power goes down between writing a bit in one stage and erasing in the next stage.

- Solution:
  - Authorization of erasing the next stage has to be memorized in a non-volatile way.
  - If power goes down, it will be possible to reset the counter at the previous value after the card is powered up again.

Anti Pull Out Mechanism

- Security done by an internal EEPROM flag for each stage
- Protection installed to prevent loss of units during an erase sequence of a stage
- Flag status change from "1" to "0" before erasing the last written stage (except C1)



C_{64}: 1 1 1 1 1 1 1 0

C_8: 1 1 1 1 1 1 1 1

Card Commands

- ❑ Reset Address Counter (RESET)
- ❑ Increment Address Counter and Read Bit (INCREMENT)
- ❑ Write Bit (WRITE)
- ❑ Present Transport Code (PRESENT)
- ❑ Write Carry and Erase Counter Stage (WRITECARRY)
- ❑ Authentication (AUTHENTICATE)

EuroChip-2 (SLE-5536)

- ❑ Downward compatible with SLE-4436
- ❑ Ciphered block chaining of the current 16 bit response to the next authentication response computation (until the next RESET)

Possible Usage of EuroChip

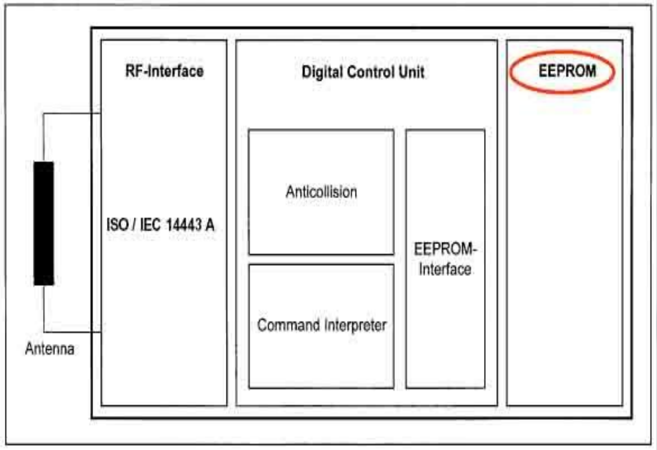
- Disposable Multi-services Phone Card
  - Vending machines
  - Cyber café
- Electronic Gift Voucher
- Electronic Purse

MIFARE

CARD & READER TECHNOLOGIES

Ultralight Block Diagram

- Total of 512 bits of memory organized into 16 pages of 4 bytes
  - 7 bytes of UID
  - 16 bits of LOCK bytes
  - 384 bits of user memory
  - 32 bits of OTP
  - 16.9 pF or 50pF

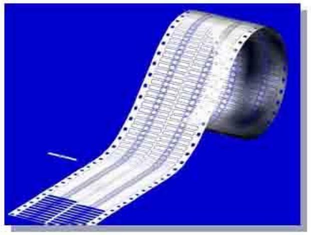


Sawn Wafer FFC

150µm thickness

MF0ICU1001W/V4D – 16.9 pF
MF0ICU1101W/V4D – 50.0 pF

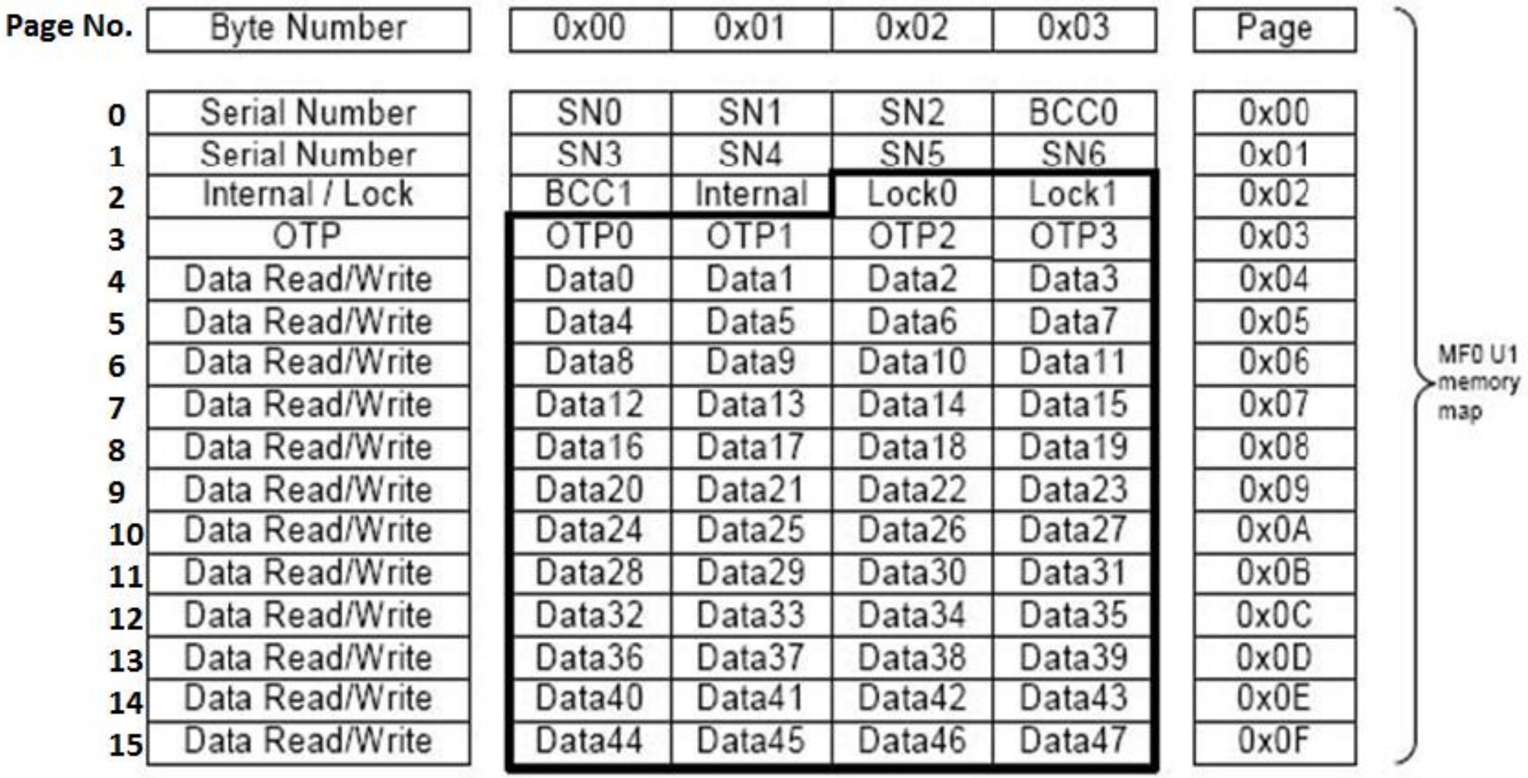
Flip Chip Package - FCP



300µm thickness

MF0FCP2U10/DH – 16.9 pF
MF0FCP2U11/DH – 50.0 pF

Ultralight Memory Map

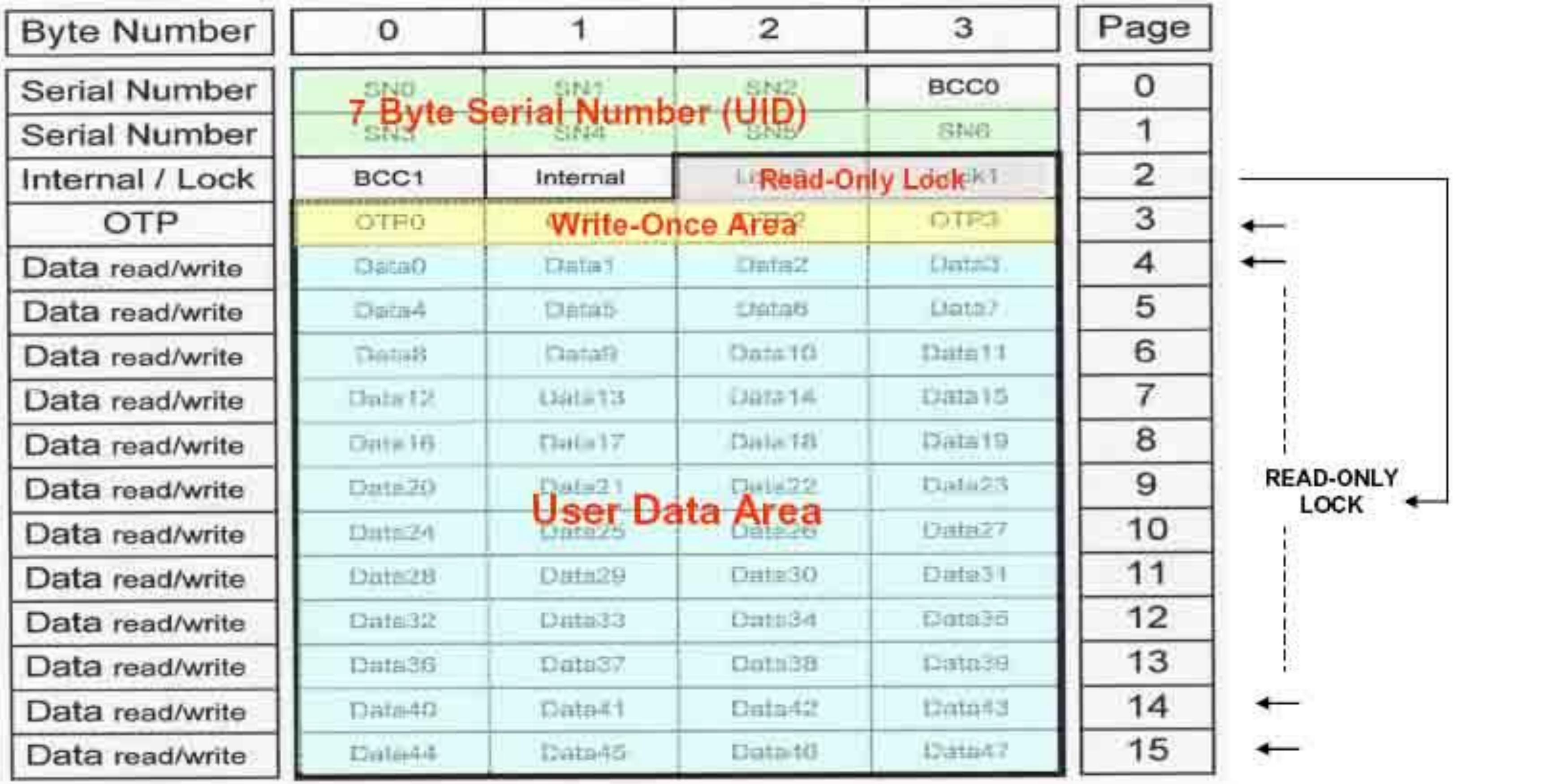


Page No.	Byte Number	0x00	0x01	0x02	0x03	Page
0	Serial Number	SN0	SN1	SN2	BCC0	0x00
1	Serial Number	SN3	SN4	SN5	SN6	0x01
2	Internal / Lock	BCC1	Internal	Lock0	Lock1	0x02
3	OTP	OTP0	OTP1	OTP2	OTP3	0x03
4	Data Read/Write	Data0	Data1	Data2	Data3	0x04
5	Data Read/Write	Data4	Data5	Data6	Data7	0x05
6	Data Read/Write	Data8	Data9	Data10	Data11	0x06
7	Data Read/Write	Data12	Data13	Data14	Data15	0x07
8	Data Read/Write	Data16	Data17	Data18	Data19	0x08
9	Data Read/Write	Data20	Data21	Data22	Data23	0x09
10	Data Read/Write	Data24	Data25	Data26	Data27	0x0A
11	Data Read/Write	Data28	Data29	Data30	Data31	0x0B
12	Data Read/Write	Data32	Data33	Data34	Data35	0x0C
13	Data Read/Write	Data36	Data37	Data38	Data39	0x0D
14	Data Read/Write	Data40	Data41	Data42	Data43	0x0E
15	Data Read/Write	Data44	Data45	Data46	Data47	0x0F

MF0 U1 memory map

Remark: Bold frame indicates user area

Ultralight Card Mapping



Byte Number	0	1	2	3	Page
Serial Number	SN0	SN1	SN2	BCC0	0
Serial Number	SN3	SN4	SN5	SN6	1
Internal / Lock	BCC1	Internal	Lock0	Lock1	2
OTP	OTP0	OTP1	OTP2	OTP3	3
Data read/write	Data0	Data1	Data2	Data3	4
Data read/write	Data4	Data5	Data6	Data7	5
Data read/write	Data8	Data9	Data10	Data11	6
Data read/write	Data12	Data13	Data14	Data15	7
Data read/write	Data16	Data17	Data18	Data19	8
Data read/write	Data20	Data21	Data22	Data23	9
Data read/write	Data24	Data25	Data26	Data27	10
Data read/write	Data28	Data29	Data30	Data31	11
Data read/write	Data32	Data33	Data34	Data35	12
Data read/write	Data36	Data37	Data38	Data39	13
Data read/write	Data40	Data41	Data42	Data43	14
Data read/write	Data44	Data45	Data46	Data47	15

UID (Serial Number)

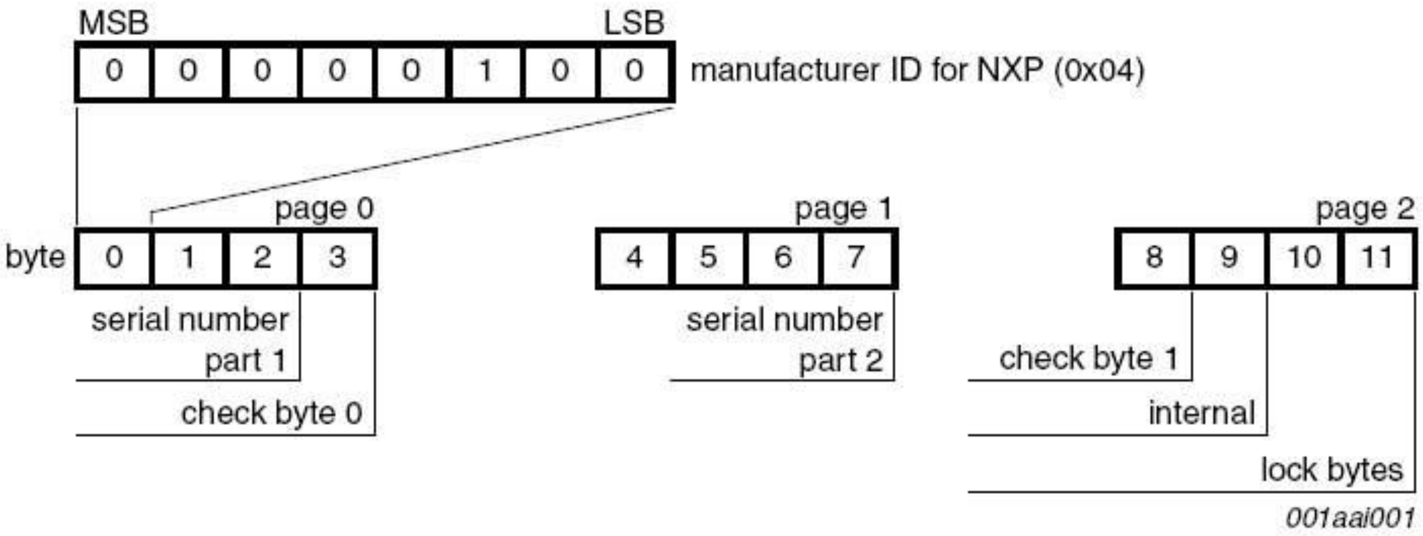
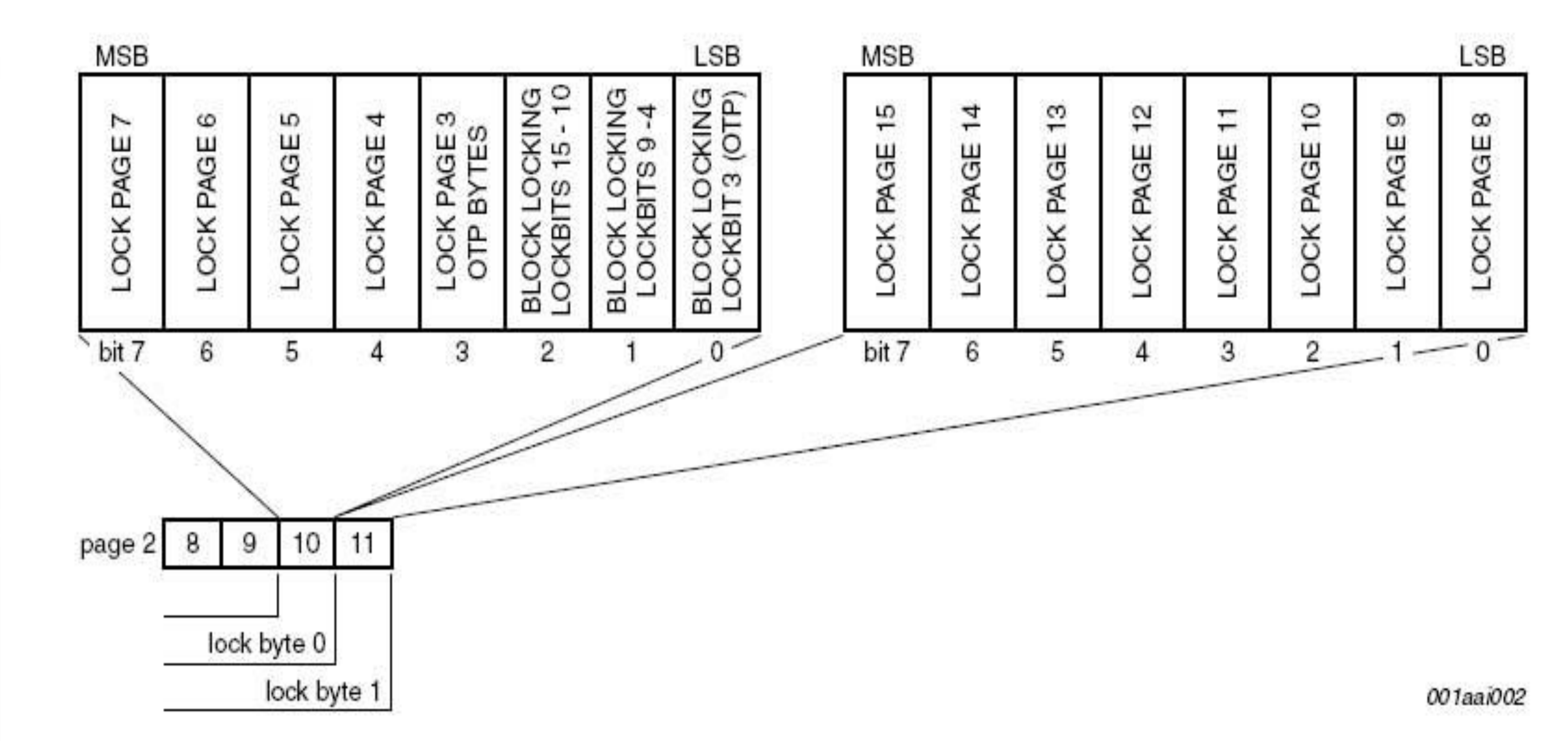


Fig 4. UID/serial number

Lock Bytes (page 2 byte 2-3)



MSB							LSB
LOCK PAGE 7	LOCK PAGE 6	LOCK PAGE 5	LOCK PAGE 4	LOCK PAGE 3 OTP BYTES	BLOCK LOCKING LOCKBITS 15 - 10	BLOCK LOCKING LOCKBITS 9 -4	BLOCK LOCKING LOCKBIT 3 (OTP)
bit 7	6	5	4	3	2	1	0

MSB							LSB
LOCK PAGE 15	LOCK PAGE 14	LOCK PAGE 13	LOCK PAGE 12	LOCK PAGE 11	LOCK PAGE 10	LOCK PAGE 9	LOCK PAGE 8
bit 7	6	5	4	3	2	1	0

page 2	8	9	10	11

lock byte 0

lock byte 1

001aai002

MiFare Ultralight Correct Usage

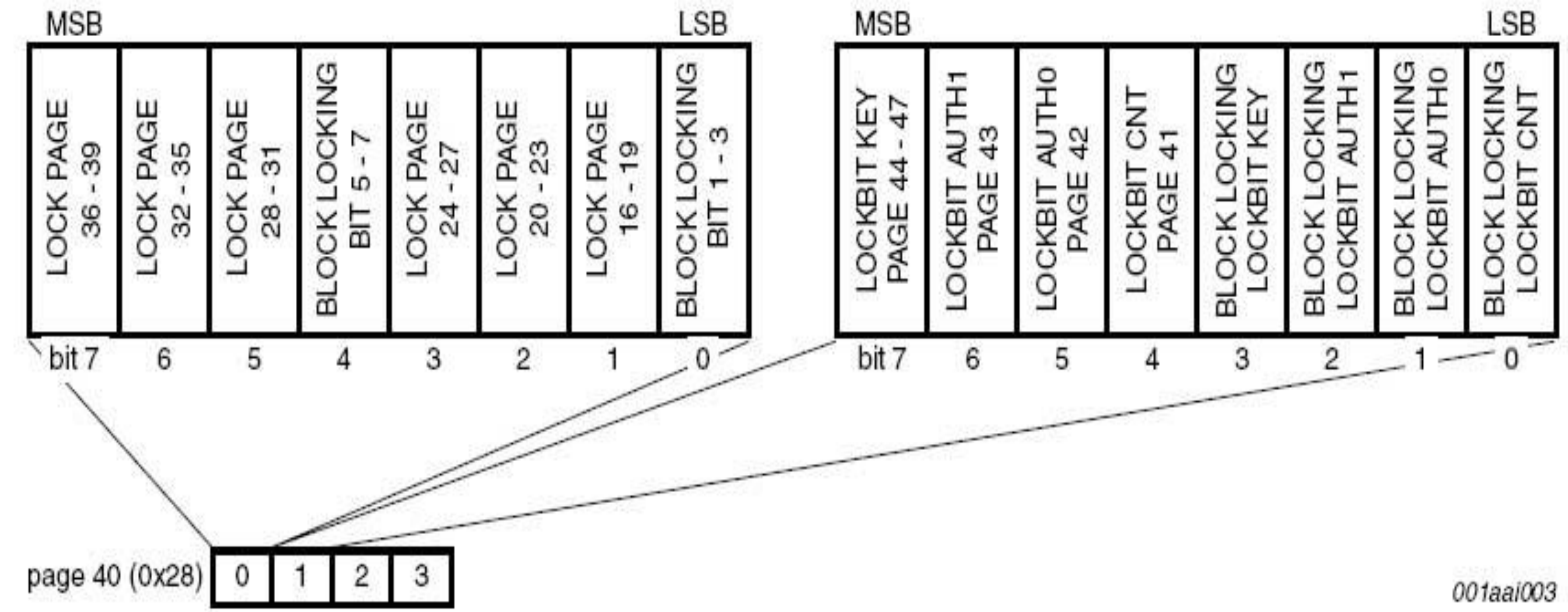
- Security Assumption
  - The UID cannot be cloned
  - The chip cannot be emulated
  - The application program cannot be tampered with
- Design Tips
  - UID to be MAC-ed by a UID MAC key
  - Static data to be MAC-ed by a static data MAC key
  - Dynamic data to be MAC-ed by a dynamic data MAC key
  - Dynamic data must be backed up in the card before data is updated

MiFare Ultralight C

- 1536 bits (192 bytes)
- First 512 bits (64 bytes) are compatible with Ultralight
- 196 bytes of memory comprising:
  - 144 bytes of user memory
  - Locking to read only (per block)
  - Card Transaction Counter, 0x0000 – 0xFFFF

Page (dec)	Page (hex)	Byte 0	Byte 1	Byte 2	Byte 3
0 – 15	00 – 0F	Compatible With MiFare Ultra-Light			
16 – 39	10 – 27	User UL2	User UL2	User UL2	User UL2
40	28	Lock UL2	Lock UL2	RFU	RFU
41	29	Counter	Counter	RFU	RFU
42	2A	AUT0	RFU	RFU	RFU
43	2B	AUT1			
44 – 47	2C – 2F	Triple DES Double Length Key			

Lock UL2



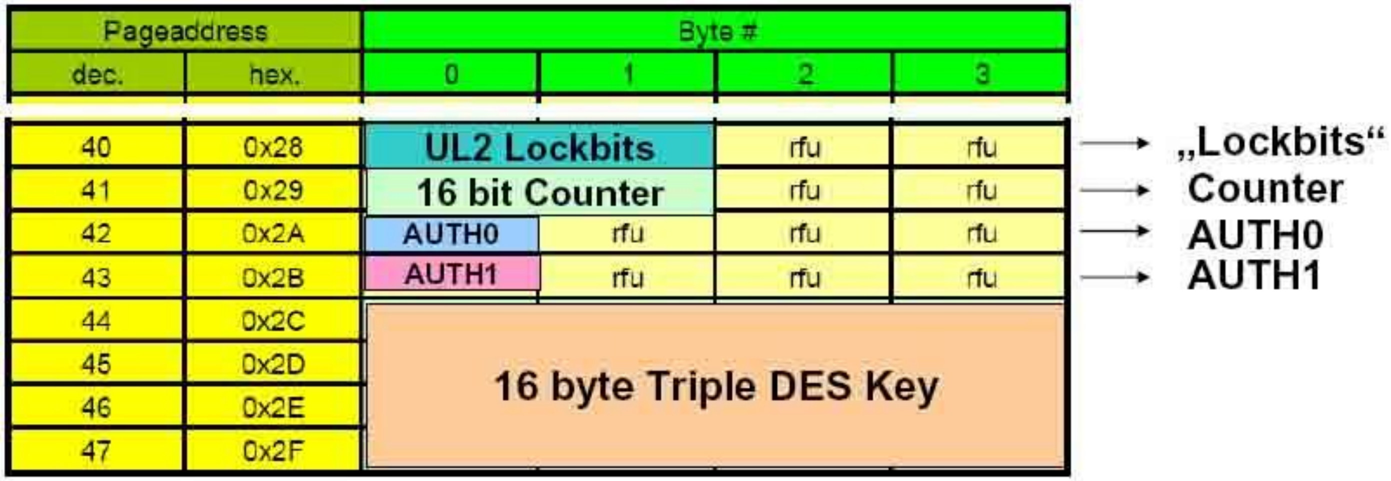
MSB							LSB
LOCK PAGE 36 - 39	LOCK PAGE 32 - 35	LOCK PAGE 28 - 31	BLOCK LOCKING BIT 5 - 7	LOCK PAGE 24 - 27	LOCK PAGE 20 - 23	LOCK PAGE 16 - 19	BLOCK LOCKING BIT 1 - 3
bit 7	6	5	4	3	2	1	0

MSB							LSB
LOCKBIT KEY PAGE 44 - 47	LOCKBIT AUTH1 PAGE 43	LOCKBIT AUTH0 PAGE 42	LOCKBIT CNT PAGE 41	BLOCK LOCKING LOCKBIT KEY	BLOCK LOCKING LOCKBIT AUTH1	BLOCK LOCKING LOCKBIT AUTH0	BLOCK LOCKING LOCKBIT CNT
bit 7	6	5	4	3	2	1	0

page 40 (0x28)	0	1	2	3

001aai003

AUTH



Pageaddress		Byte #				
dec.	hex.	0	1	2	3	
40	0x28	UL2 Lockbits		rfu	rfu	„Lockbits“
41	0x29	16 bit Counter		rfu	rfu	Counter
42	0x2A	AUTH0	rfu	rfu	rfu	AUTH0
43	0x2B	AUTH1	rfu	rfu	rfu	AUTH1
44	0x2C	16 byte Triple DES Key				
45	0x2D					
46	0x2E					
47	0x2F					

AUTH0: Defines first Page, which requires an Authentication.

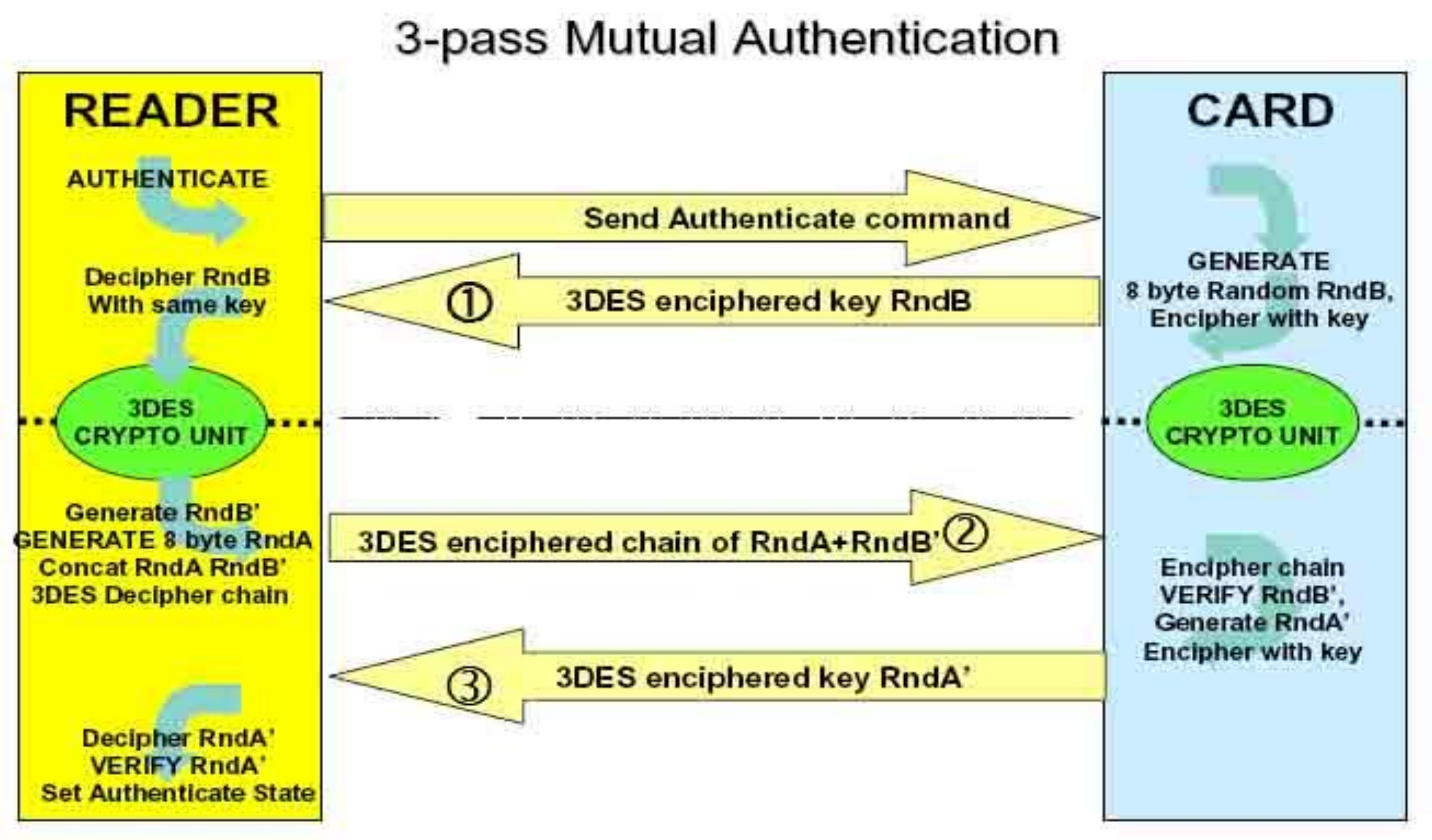
AUTH1:
bit0=1: Only Write requires Authentication
bit0=0: Read and Write requires an Authentication
bit1~7: Negligible

AUTH0 = 05hex
AUTH1 = 00hex
} **Reading and writing Pages from 05hex to 27hex require an Authentication.**

Counter

- Counter, Page 40 (29 hex)
  - Initially set to 00 00 hex
  - Can be set once to any start value using the write command (Write or C.Write)
  - Can only be incremented (using Write or C. Write)
  - Minimum Increment is 1 (00 00 00 01 hex)
  - Maximum Increment is 15 (00 00 00 0F hex)
  - Can be locked
  - Counts up to max FF FF hex

Mutual Authentication



3-pass Mutual Authentication

READER

AUTHENTICATE

Decipher RndB
With same key

3DES
CRYPTO UNIT

Generate RndB'
GENERATE 8 byte RndA
Concat RndA RndB'
3DES Decipher chain

Decipher RndA'
VERIFY RndA'
Set Authenticate State

Send Authenticate command

① 3DES enciphered key RndB

3DES enciphered chain of RndA+RndB' ②

③ 3DES enciphered key RndA'

CARD

GENERATE
8 byte Random RndB,
Encipher with key

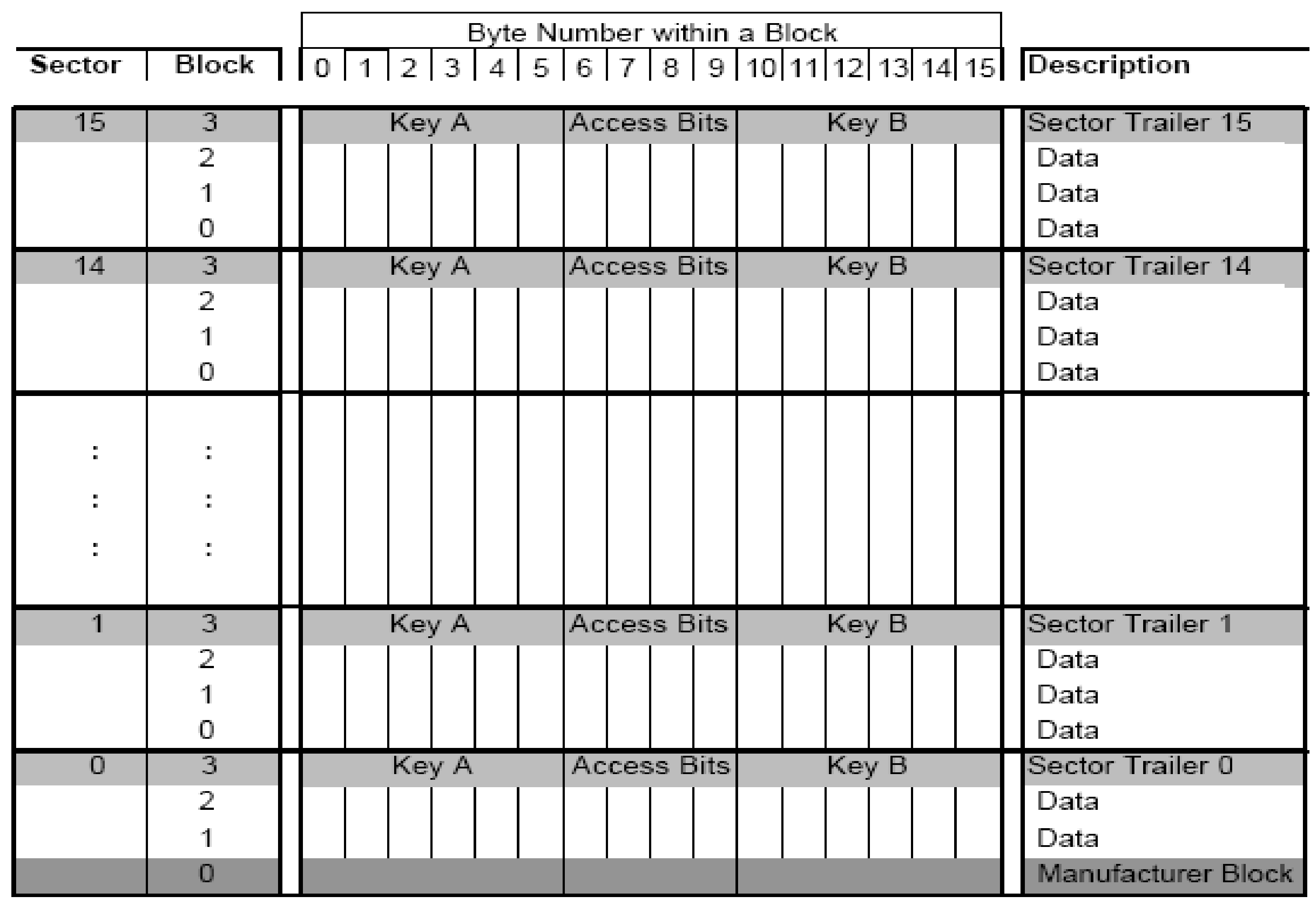
3DES
CRYPTO UNIT

Encipher chain
VERIFY RndB',
Generate RndA'
Encipher with key

MiFare Ultralight C Correct Usage

- Security Assumption
  - Application program cannot be tampered with
- Design Tips
  - UID to be MAC-ed by a UID MAC key
  - Static data to be MAC-ed by a static data MAC key
  - Dynamic data to be MAC-ed by a dynamic data MAC key
  - Dynamic data must be backed up in the card before data is updated
  - MAC must be verified before usage of data; counter incremented and new MAC computed
  - If stored value is used, a balance MAC is required to protect the balance
  - Debit terminal PSAM can only compute a balance MAC with a lower balance
  - After reloading, new balance MAC is computed by remote the host HSM; or if offline credit, it can only be computed after verification that the same balance has been debited from the cashier card

MiFare 1 Kbytes

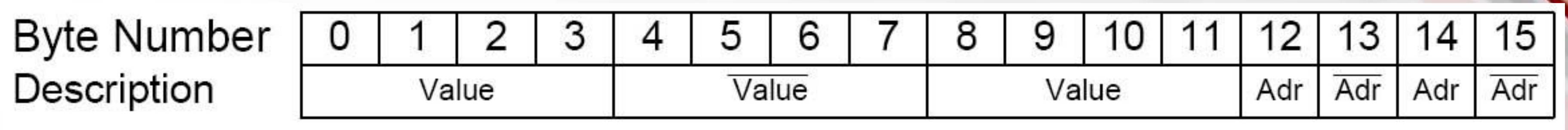


		Byte Number within a Block																
Sector	Block	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Description
15	3	Key A						Access Bits				Key B						Sector Trailer 15
	2																	Data
	1																	Data
	0																	Data
14	3	Key A						Access Bits				Key B						Sector Trailer 14
	2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

Page 0, Block 0 - Manufacturer Block

- Read-only data block
- Chip serial number (4 bytes)
- LRC of serial number (1 byte)
- Chip data (4 bytes)
  - Memory size (1 byte)
  - Chip type (2 bytes)
  - Chip version (‘C’) (1 byte)
- Batch number (3 bytes)
- Date (yy,week) (4 bytes)

Value Block



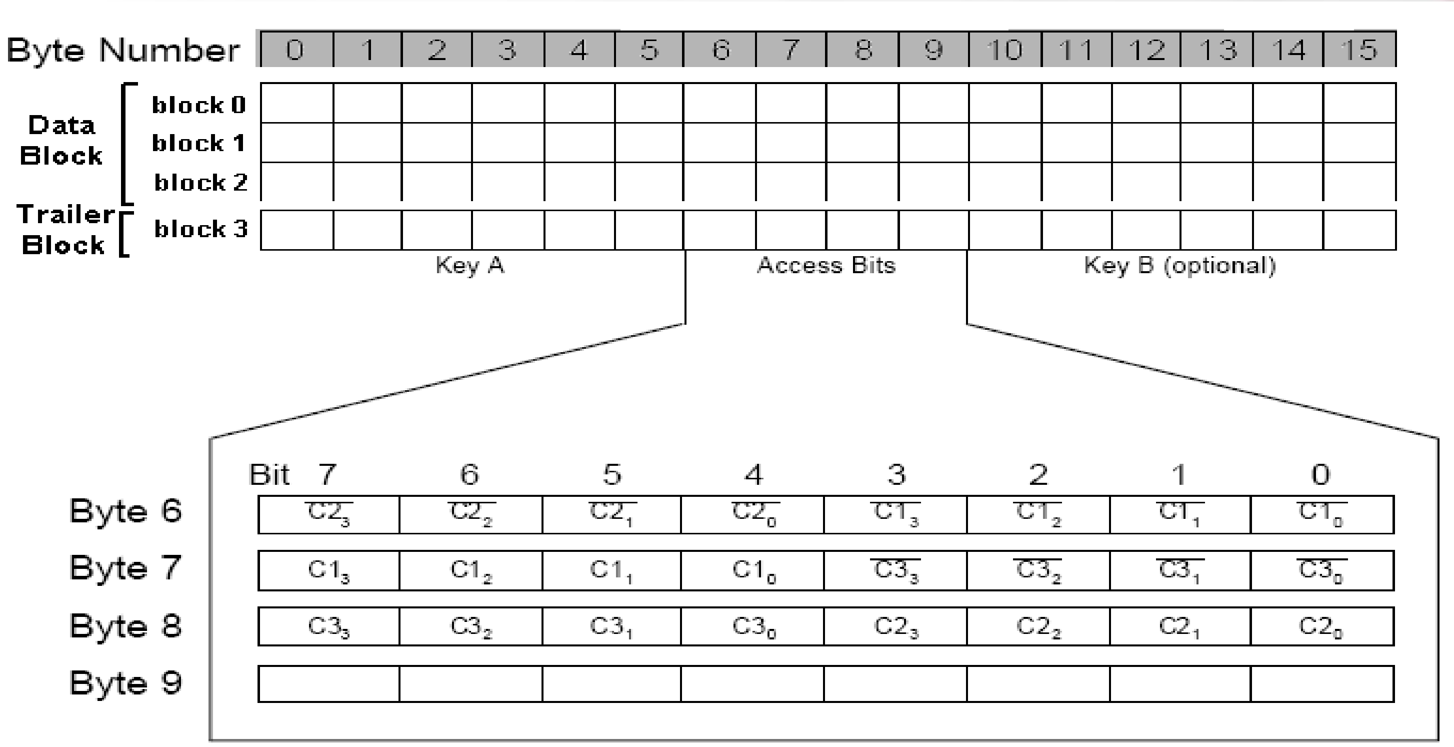
Byte Number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Description	Value				$\overline{\text{Value}}$				Value				Adr	$\overline{\text{Adr}}$	Adr	$\overline{\text{Adr}}$

- The value block is identified by a complementary data, otherwise it is a data block.
- Addr data is not evaluated by the chip and is for application use (eg. pointer to backup)
- Personalization responsibility is needed to ensure initialization in a complementary format.
- Subsequent value complements are handled by the chip.
- Subtract value (debit) and add value (credit) operations can only be performed on the Value Block.

Value Block's Content

- 0 = 0000 0000 FFFF FFFF 0000 0000
- 1 = 0100 0000 FEFF FFFF 0100 0000
- -1 = FFFF FFFF 0000 0000 FFFF FFFF
- -2 = FEFF FFFF 0100 0000 FEFF FFFF
- Value is a signed word (4 bytes)
- Minimum value is –2147483648 (eg.0000 0000 0000 0080)
- Wrap-around is NOT possible

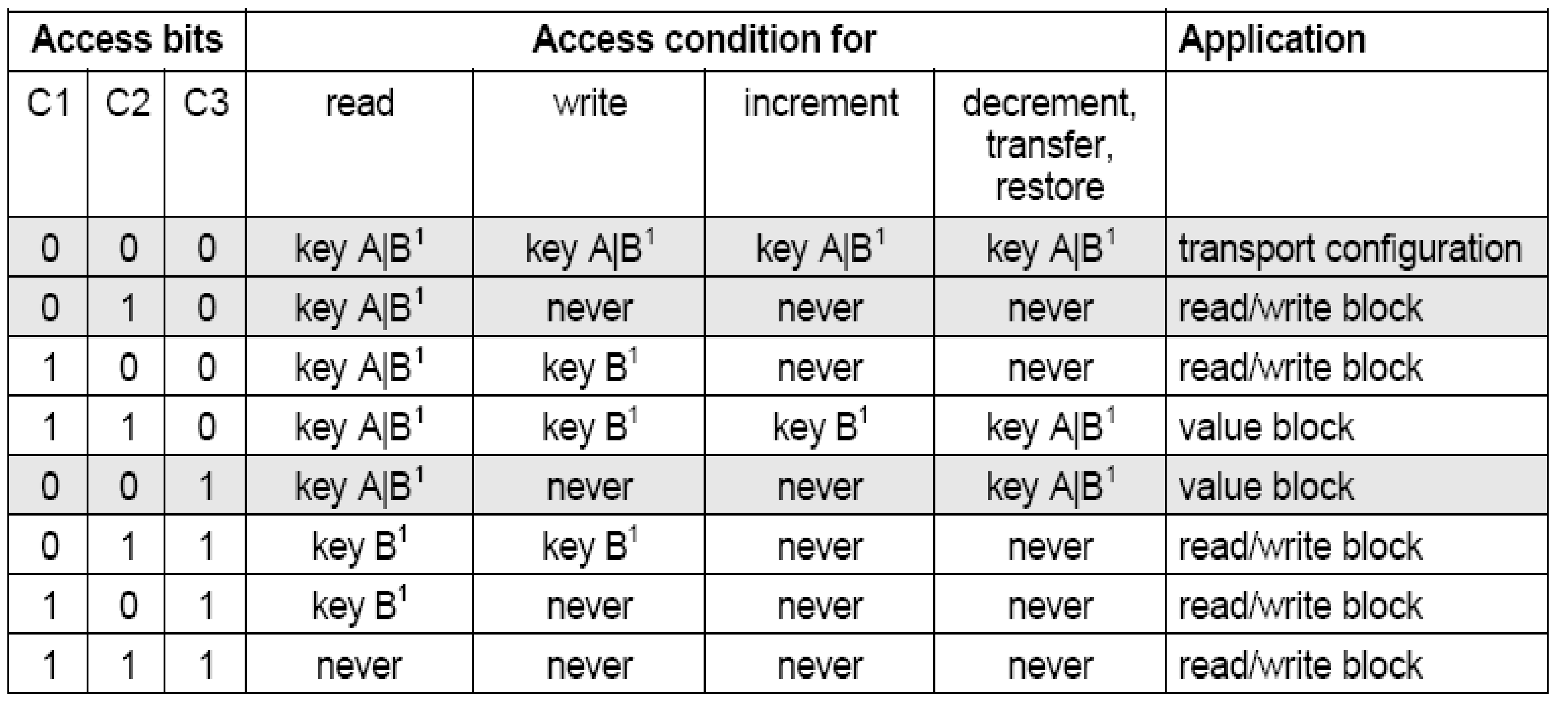
Trailer Block



	Bit 7	6	5	4	3	2	1	0
Byte 6	$\overline{C2_3}$	$\overline{C2_2}$	$\overline{C2_1}$	$\overline{C2_0}$	$\overline{C1_3}$	$\overline{C1_2}$	$\overline{C1_1}$	$\overline{C1_0}$
Byte 7	$C1_3$	$C1_2$	$C1_1$	$C1_0$	$\overline{C3_3}$	$\overline{C3_2}$	$\overline{C3_1}$	$\overline{C3_0}$
Byte 8	$C3_3$	$C3_2$	$C3_1$	$C3_0$	$C2_3$	$C2_2$	$C2_1$	$C2_0$
Byte 9								

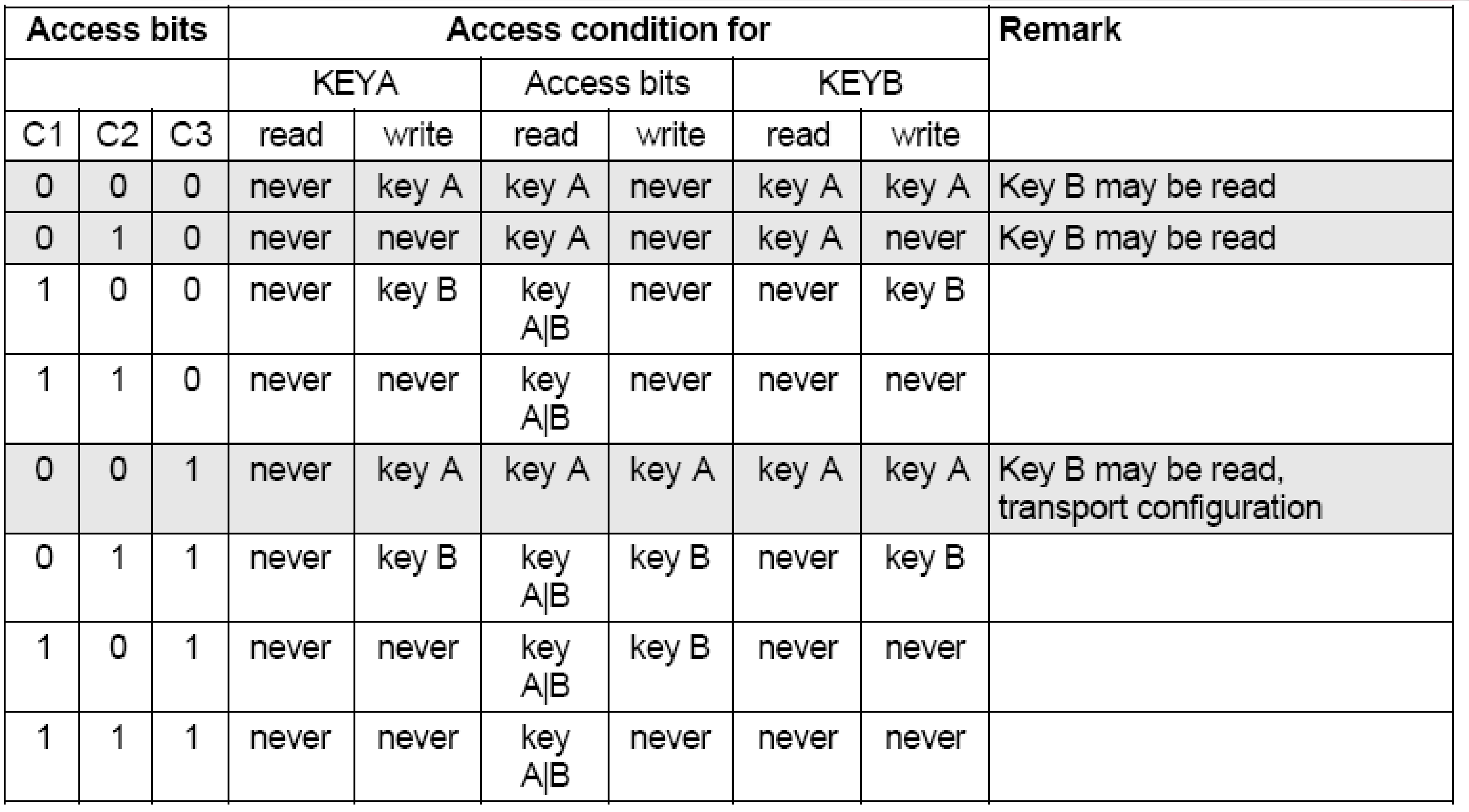
Access Bits	Valid Commands		Block	Description
$C1_3$ $C2_3$ $C3_3$	read, write	→	3	sector trailer
$C1_2$ $C2_2$ $C3_2$	read, write, increment, decrement, transfer, restore	→	2	data block
$C1_1$ $C2_1$ $C3_1$	read, write, increment, decrement, transfer, restore	→	1	data block
$C1_0$ $C2_0$ $C3_0$	read,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

Access Modes for Data/Value Block



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

Access Modes for Trailer Block



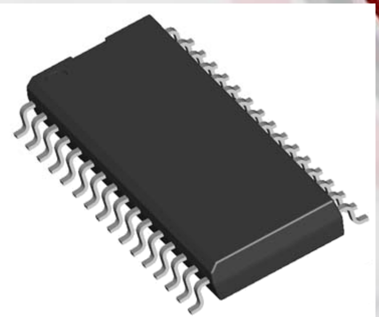
Access bits			Access condition for						Remark
			KEYA		Access bits		KEYB		
C1	C2	C3	read	write	read	write	read	write	
0	0	0	never	key A	key A	never	key A	key A	Key B may be read
0	1	0	never	never	key A	never	key A	never	Key B may be read
1	0	0	never	key B	key A|B	never	never	key B	
1	1	0	never	never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

Easykey.exe

MiFare Correct Usage

- Security Assumption
  - Application program cannot be tampered with
- Design Tips
  - UID to be MAC-ed by a UID MAC key
  - Key diversification possible only if the MAC is correct
  - Static data to be MAC-ed by a static data MAC key
  - Dynamic data to be MAC-ed by a dynamic data MAC key
  - Dynamic data must be backed up in the card before data is updated
  - MAC must be verified before usage of data; counter decremented and new MAC computed
  - Stored value is protected by a balance MAC
  - Debit terminal PSAM can only compute a balance MAC with a lower balance
  - After reloading, new balance MAC is computed by the remote host HSM; or if offline credit, it can only be computed after verification that the same balance has been debited from the cashier card.

MiFare Reader ASIC



Reader ICs	R/W Distance	Host Interface	Card Interface	Data Rates
MF RC500	100 mm	Parallel	ISO 14443A	---
MF RC530	100 mm	Parallel, SPI	ISO 14443A	Up to 424 kbaud
MF RC531	100 mm	Parallel, SPI	ISO 14443A&B	Up to 424 kbaud
CL RC632	100 mm	Parallel, SPI	ISO 14443A&B	Up to 424 kbaud

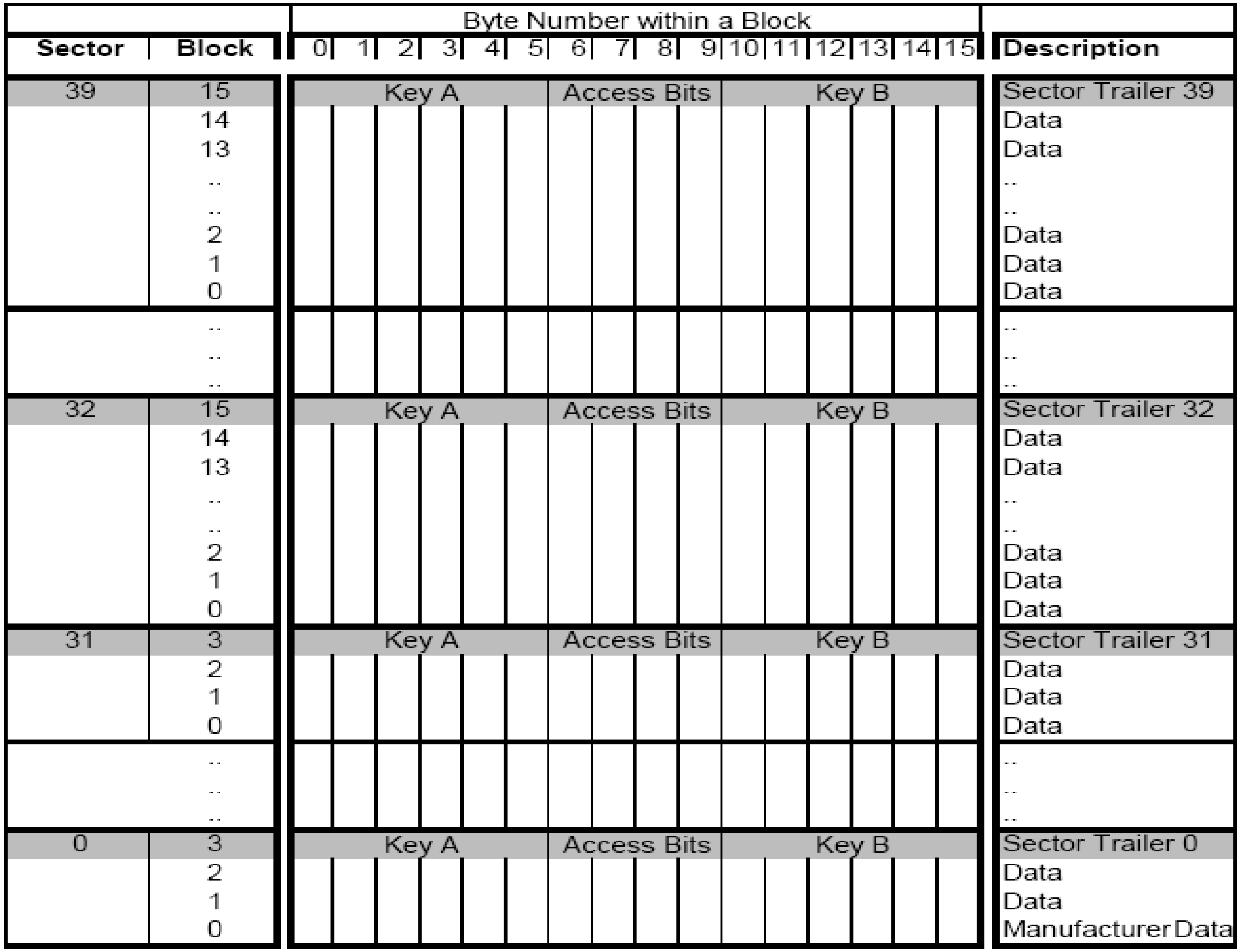
MiFare 4 Kbytes

Sector 0 - 31

16 bytes / block
4 blocks / page

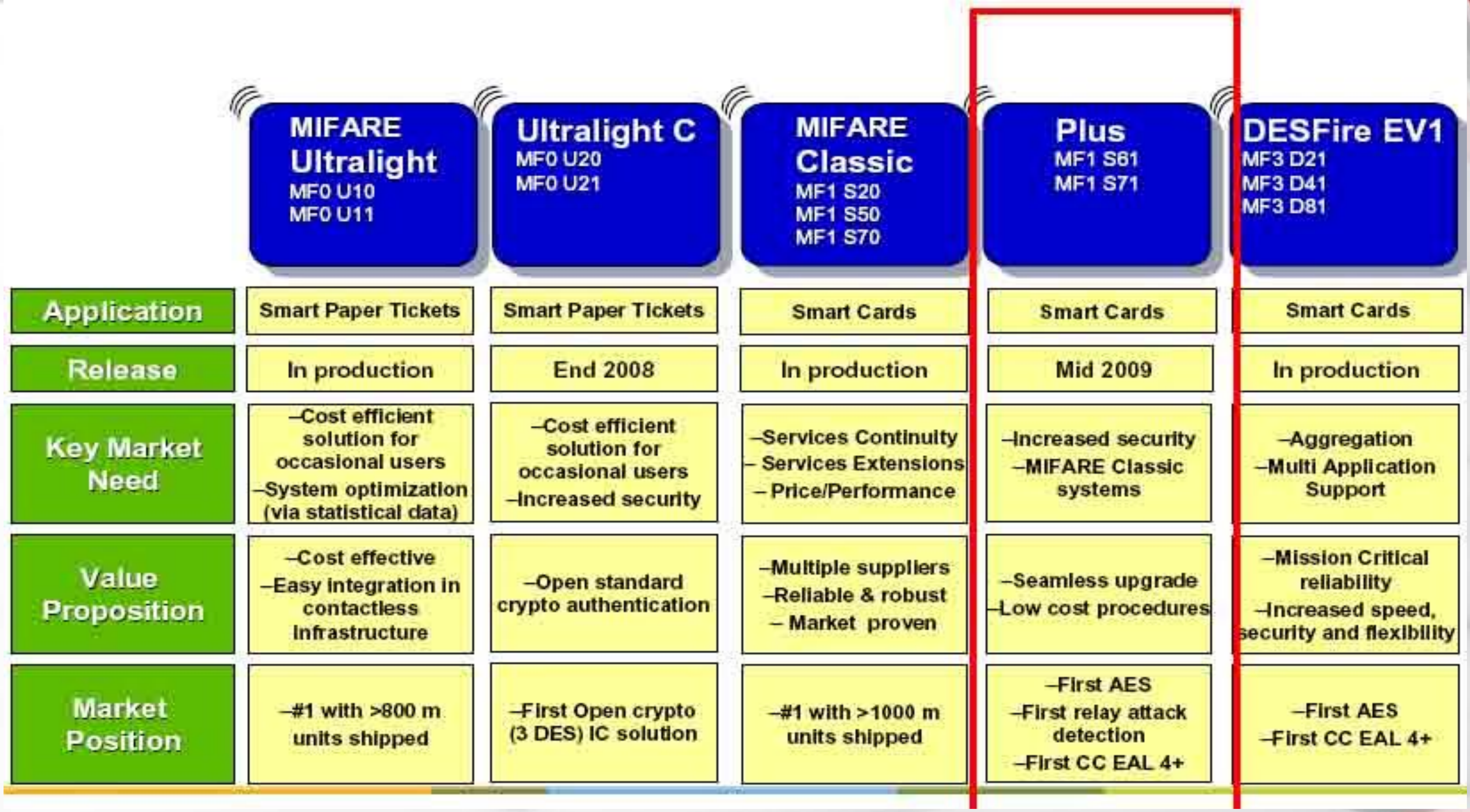
Sector 32 – 39
16 bytes / block
16 blocks / page

16 * 4 * 32 pages
+16*16*8pages
= 4096 bytes



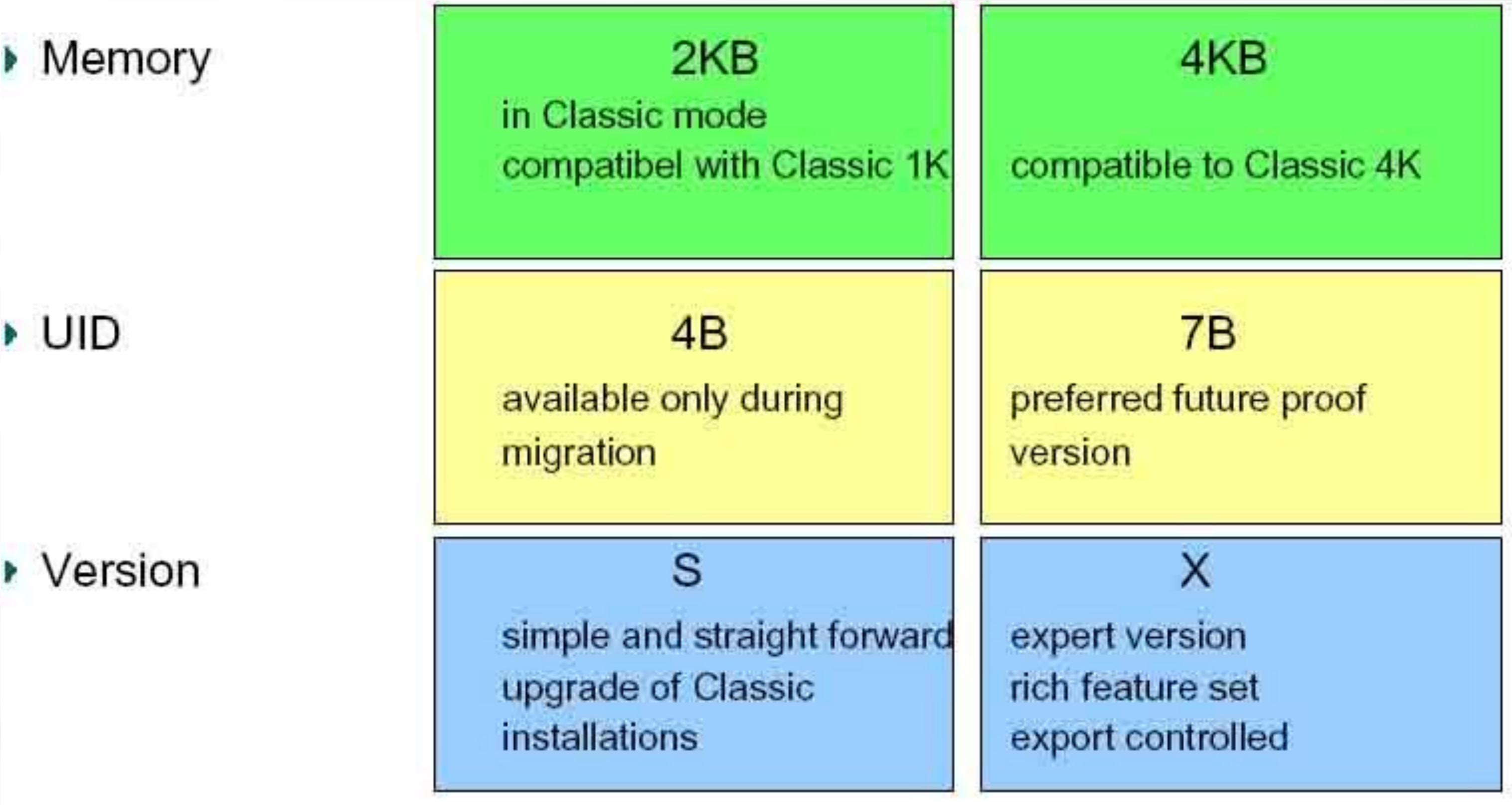
		Byte Number within a Block																
Sector	Block	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Description
39	15	Key A						Access Bits				Key B						Sector Trailer 39
	14																	Data
	13																	Data
	..																	..
	..																	..
	2																	Data
	1																	Data
	0																	Data
	..																	..
	..																	..
	..																	..
32	15	Key A						Access Bits				Key B						Sector Trailer 32
	14																	Data
	13																	Data
	..																	..
	..																	..
	2																	Data
	1																	Data
	0																	Data
31	3	Key A						Access Bits				Key B						Sector Trailer 31
	2																	Data
	1																	Data
	0																	Data
	..																	..
	..																	..
	..																	..
0	3	Key A						Access Bits				Key B						Sector Trailer 0
	2																	Data
	1																	Data
	0																	ManufacturerData

MiFare Plus



	MIFARE Ultralight MF0 U10 MF0 U11	Ultralight C MF0 U20 MF0 U21	MIFARE Classic MF1 S20 MF1 S50 MF1 S70	Plus MF1 S81 MF1 S71	DESFire EV1 MF3 D21 MF3 D41 MF3 D81
Application	Smart Paper Tickets	Smart Paper Tickets	Smart Cards	Smart Cards	Smart Cards
Release	In production	End 2008	In production	Mid 2009	In production
Key Market Need	–Cost efficient solution for occasional users –System optimization (via statistical data)	–Cost efficient solution for occasional users –Increased security	–Services Continuity – Services Extensions – Price/Performance	–Increased security –MIFARE Classic systems	–Aggregation –Multi Application Support
Value Proposition	–Cost effective –Easy integration in contactless infrastructure	–Open standard crypto authentication	–Multiple suppliers –Reliable & robust – Market proven	–Seamless upgrade –Low cost procedures	–Mission Critical reliability –Increased speed, security and flexibility
Market Position	–#1 with >800 m units shipped	–First Open crypto (3 DES) IC solution	–#1 with >1000 m units shipped	–First AES –First relay attack detection –First CC EAL 4+	–First AES –First CC EAL 4+

MiFare Plus Family



Memory	2KB in Classic mode compatibel with Classic 1K	4KB compatible to Classic 4K
UID	4B available only during migration	7B preferred future proof version
Version	S simple and straight forward upgrade of Classic installations	X expert version rich feature set export controlled

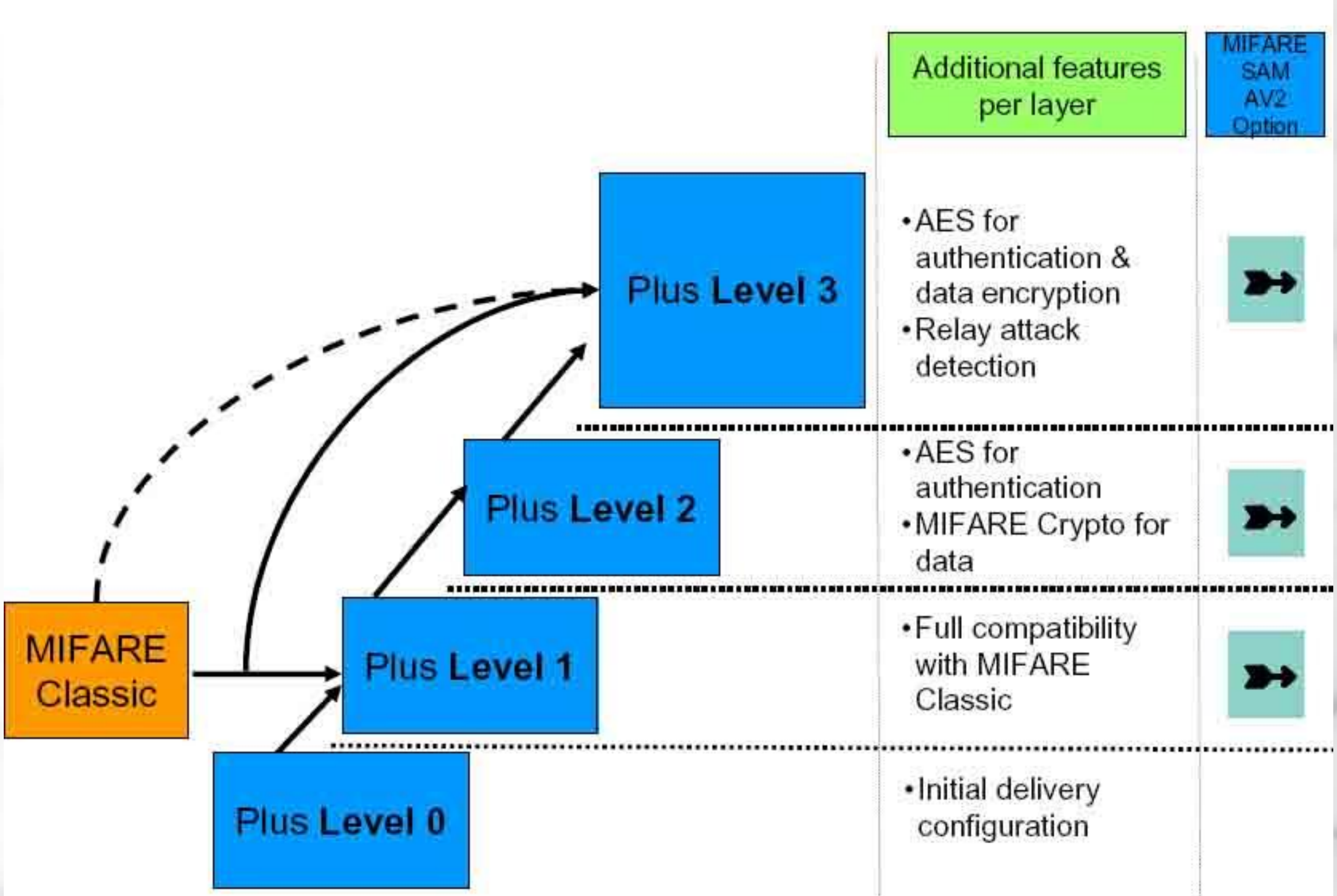
MiFare Plus General Features

- 2 Kbyte or 4 Kbyte versions
- Downward compatible with MiFare 4K,1K and MiFare Mini
- ISO-14443 A 4 bytes or 7 bytes of UID; or 3 bytes of random ID
    - Multi-sector authentication; multi-block read / write
    - As long as sectors have the same AES key not necessarily consecutive sectors but just consecutive operation
- Applicable to security levels 2 and 3
- MiFare crypto1 keys (2x48 bits sectors) or AES 2x128 bits / sector
- 500K write cycles, EAL4+, configurable access conditions
- Speed = up to 848 Kbps

MiFare Plus Security Features

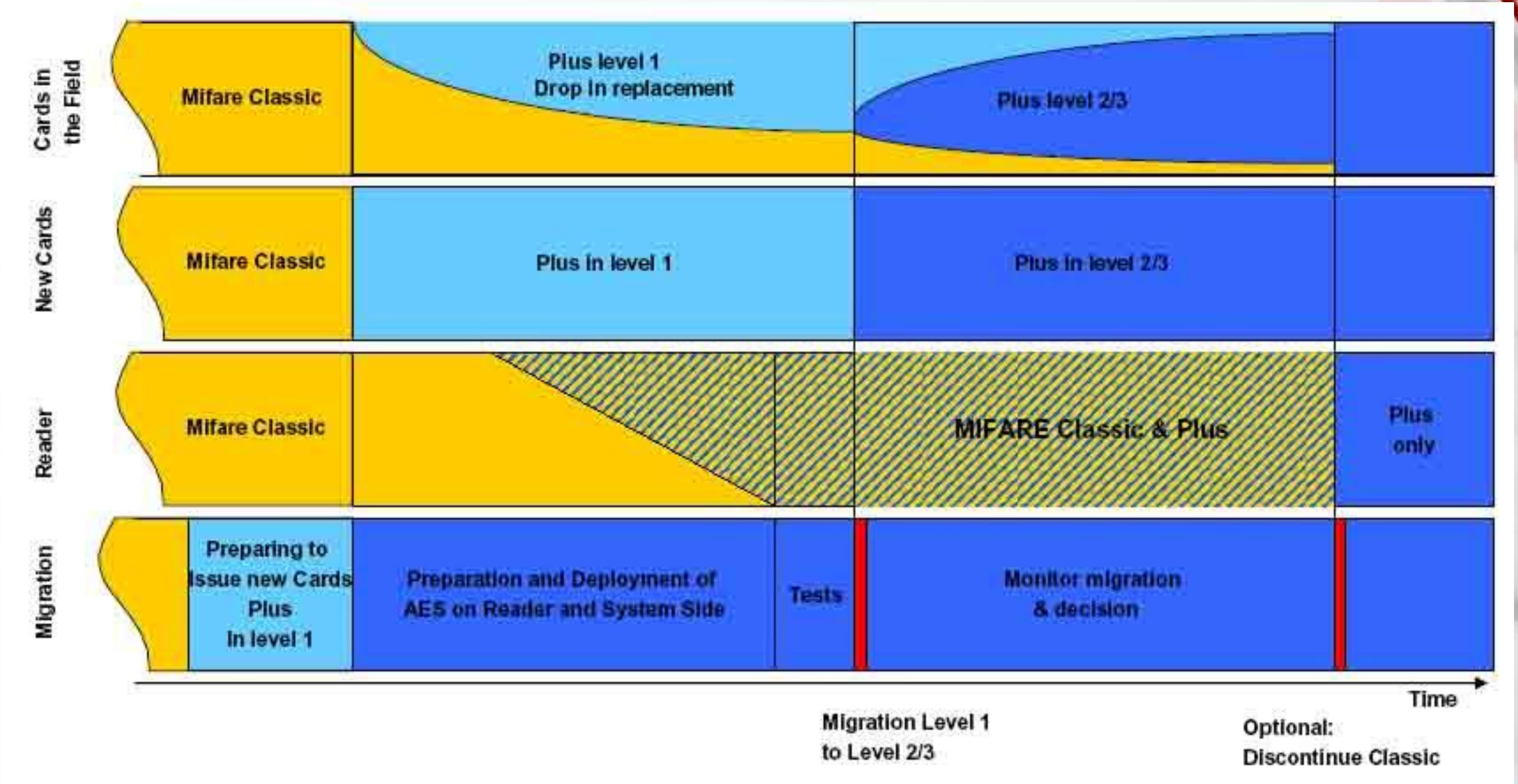
- 4 security levels
- Level 0 – Initial delivery configuration
- Level 1 – MiFare 4K, 1K and mini backward compatible
- Level 2 – AES authentication, MiFare crypto1 data confidentiality
  - Anti-tearing only for AES key update
- Level 3 – AES authentication, confidentiality and integrity
  - Anti-tearing for AES key update and trailer
- Can dynamically switch to higher level security through authentication with higher security authentication key

MiFare Plus Security Features



	Additional features per layer	MIFARE SAM AV2 Option
Plus Level 3	• AES for authentication & data encryption • Relay attack detection	➔
Plus Level 2	• AES for authentication • MIFARE Crypto for data	➔
Plus Level 1	• Full compatibility with MIFARE Classic	➔
Plus Level 0	• Initial delivery configuration	

Typical Migration Scenarios



Security Level 1

- Use Write Perso to change data and default AES keys (for better security management)
- Use Commit Perso to enable effect of written keys
  - Configuration, Card Master, Level 2 & 3 Switch Keys

Security Level 2

- Each sector contains 2 crypto1 keys; 2 AES keys
- AES authentication generates a session key, which is then XORed with the crypto1 key to perform crypto1 authentication
- To switch from L2 to L3, use the Security Level 3 Switch Key
- Changing back to a lower security level is not possible
- Changing AES keys and Configuration Blocks is possible
- Multi-block (1 to 3 blocks) read and write is possible

Security Level 3

- Random ID is available.
- An integrity and a confidentiality session key is generated after an AES authentication.
- Read command is MACed but can also be configured as not MACed for performance reasons. Proximity check can still prevent tampering.
- Write command is always MACed.
- Each block can be configured to allow/disallow plain communication.
- The reader can decide to retrieve MAC to be included in the response.

MiFare Plus Correct Usage

- Security Assumption
  - Application program cannot be tampered with
- Design Tips
  - Card is only secured if it operates in security level 3 with secured messaging (SM)
  - A secured card does not imply a secured application, therefore security design must be correct
  - SAM must be used to authenticate the card, and to generate and verify SM
  - SAM must verify generated SM for debit, and verify the response followed by generating a debit certificate for back-end verification
  - SM credit command must be generated by the backend, and the response, verified
  - If offline credit, SM for credit must only be generated after verifying that the cashier card is debited. The credit response is verified before generating a credit signature

Questions?