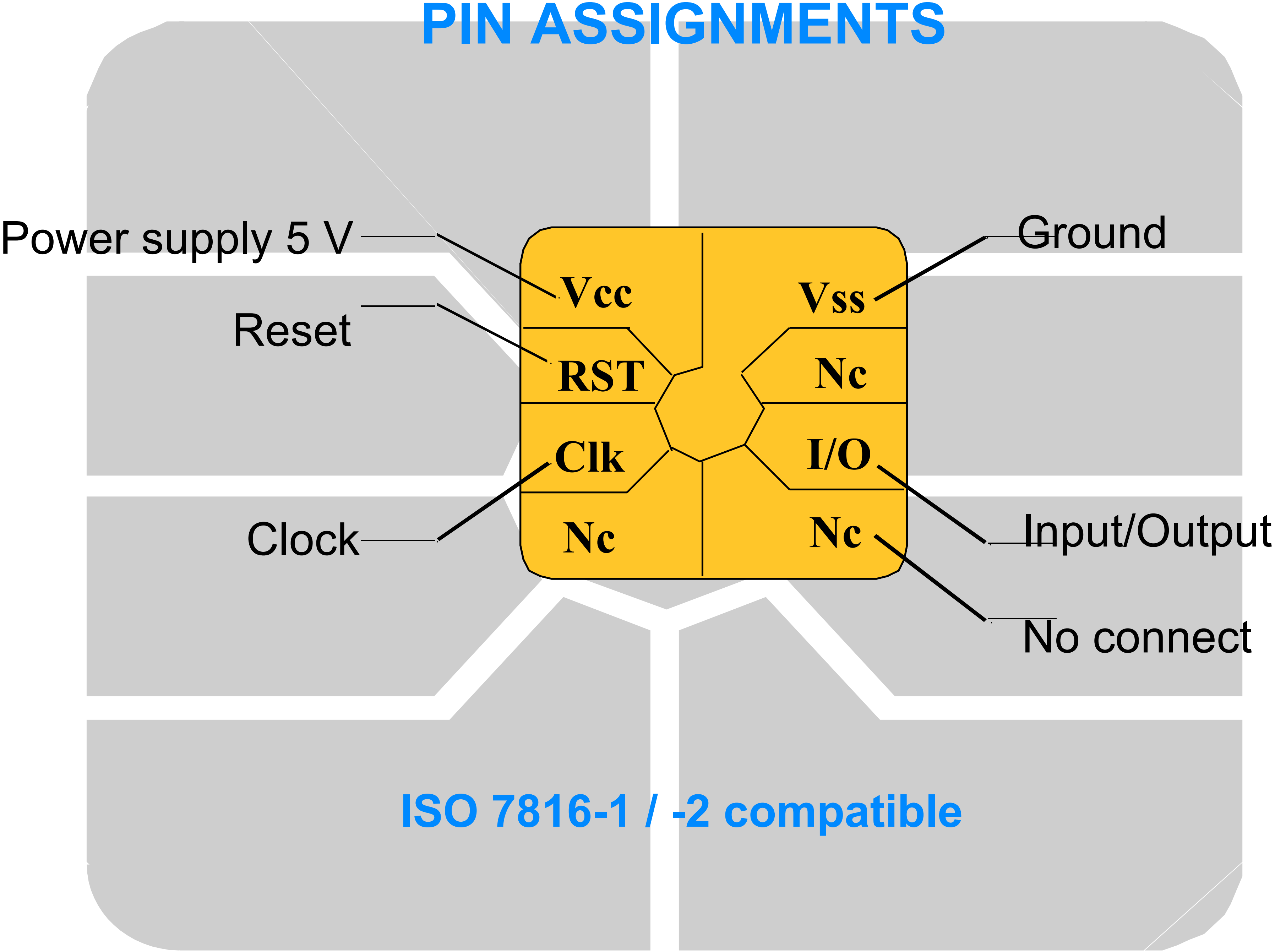
2ND GENERATION TELEPHONE CARD - SLE-4436

- 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



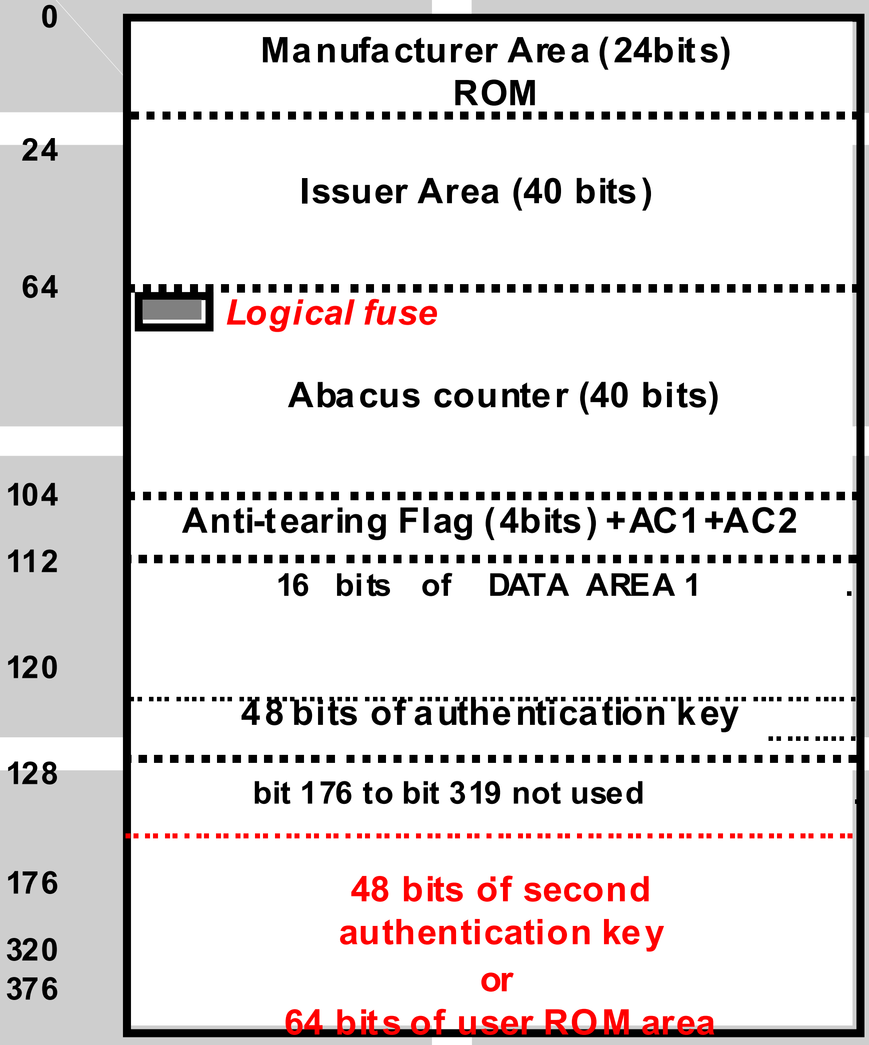
ISO 7816-1 / -2 compatible

T&C Technologies

ELECTRICAL CHARACTERISTICS

- 5v supply voltage (VCC)
- Low power consumption, < 5mA
- Compatible with SLE-4406
- Operating range : - 35蚓 to + 80蚓
- Ten years minimum data retention
- 100K erase write cycle
- EEPROM programming time 5 ms

Memory Organisation



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

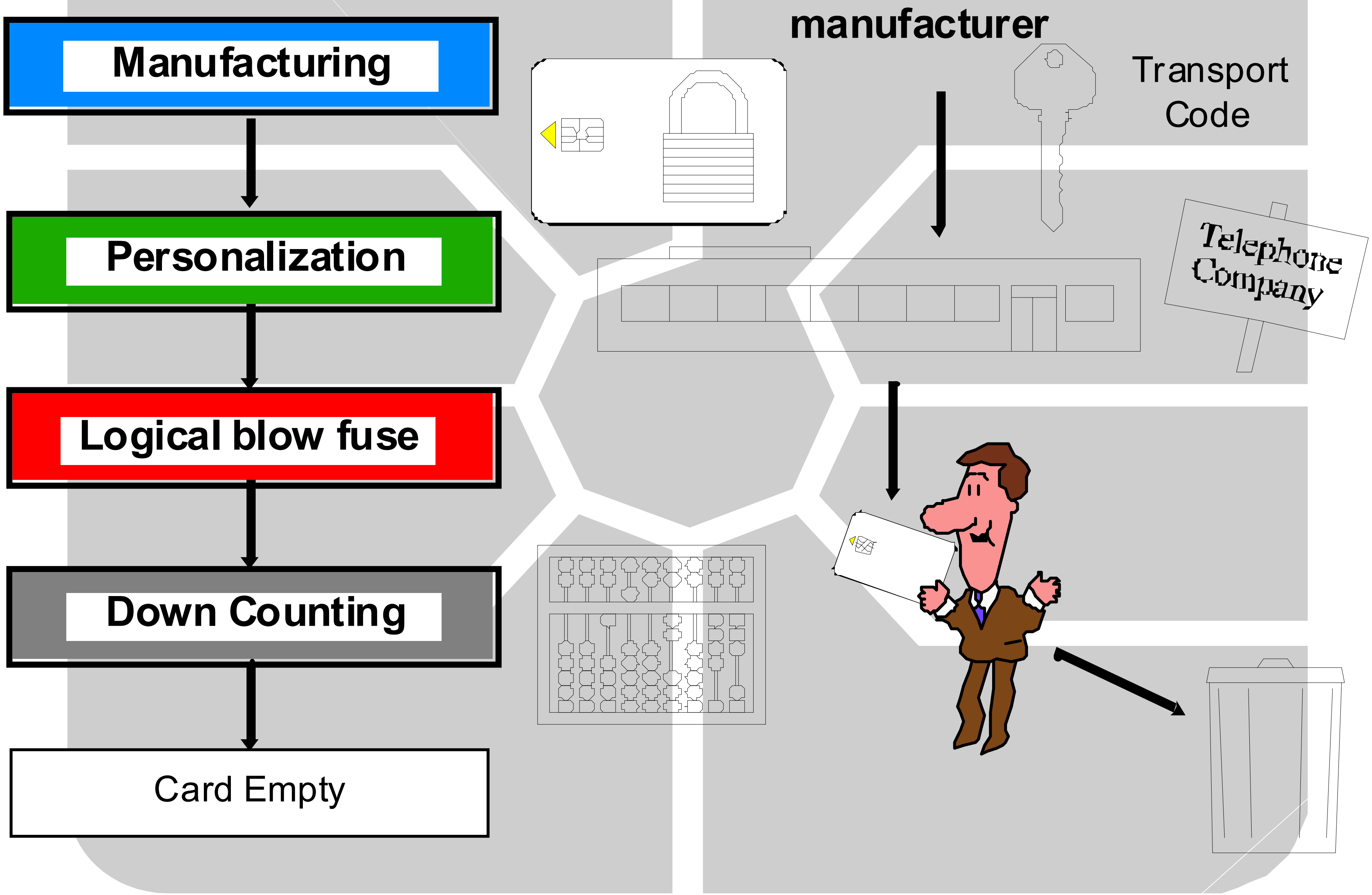
ADDITIONAL FEATURES COMPARED TO THE SLE-4406

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

ADDITIONAL FEATURES PURPOSE

- Authentication algorithm
  - To authenticate the card by the terminal
  - To avoid fabrication of counterfeited card
- Anti Pull-out protection
  - To avoid any lost 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

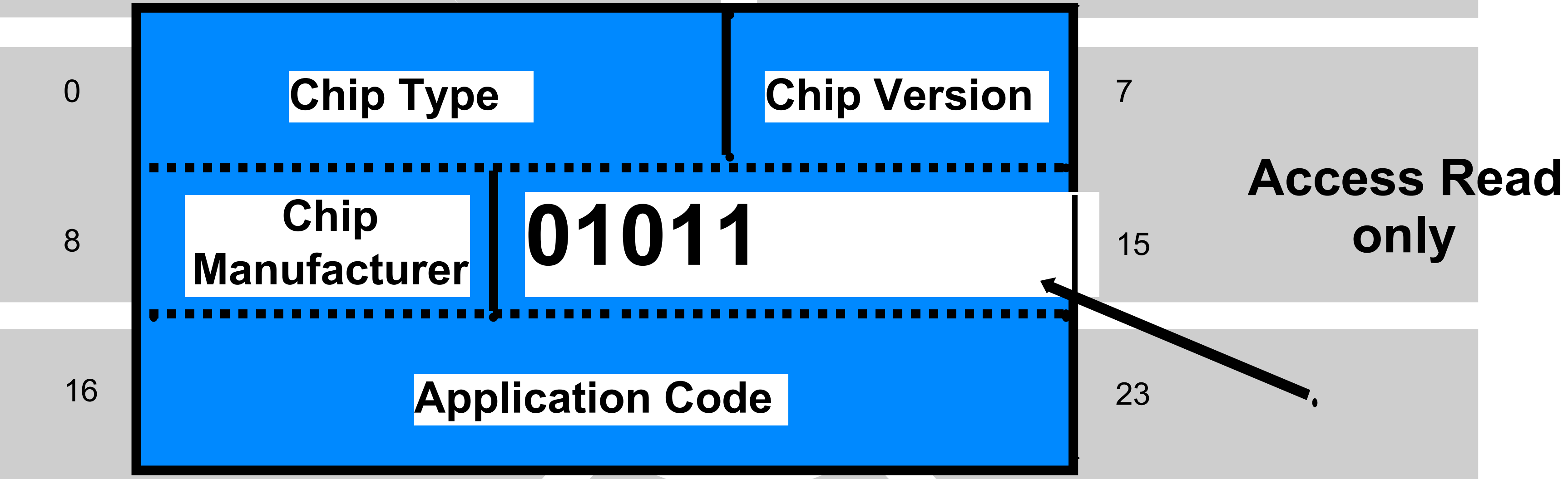
Personalization

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

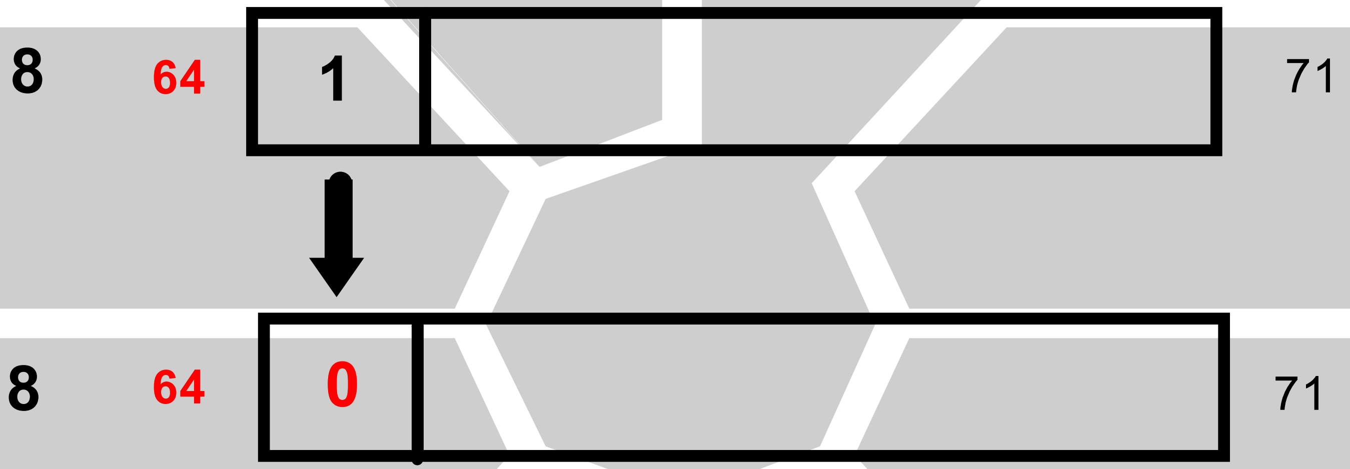
23

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

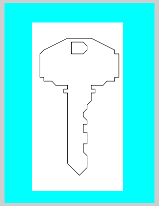
This is irreversible

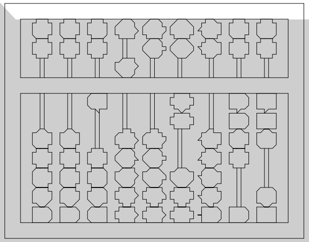
BEFORE AND AFTER FUSE BLOW

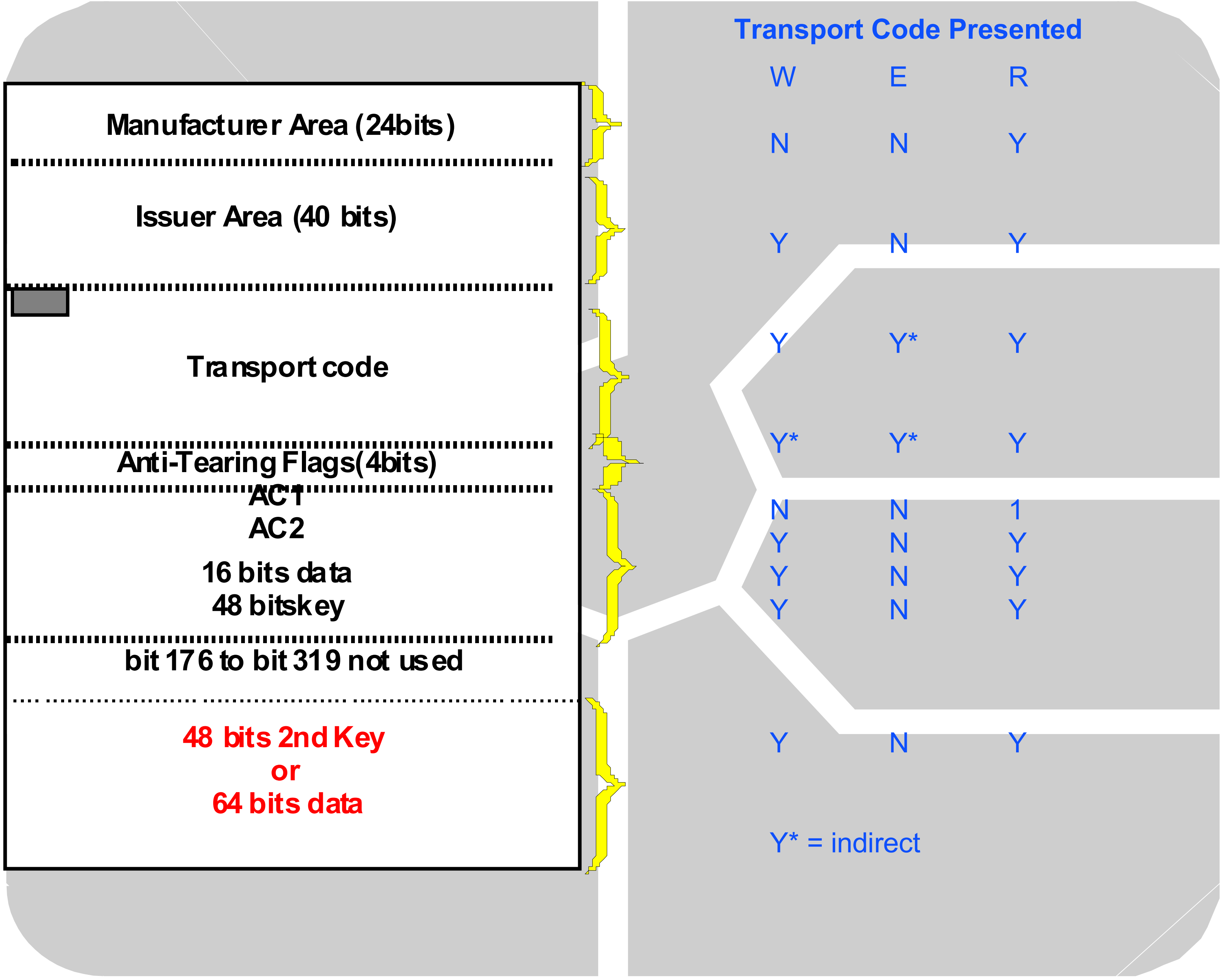
- Before (Personalization Mode)
  - 24-bits Manufacturing information (read only)
  - Protected by transport code
  - 7 attempts to present transport code then the card is useless
  - Loadable counter with value 0-33,352
- After (**Count Down Mode**)
  - Down Counter from loaded value to zero
  - Issuer and manufacturer informations is read only
  - No access to key area after the fuse 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

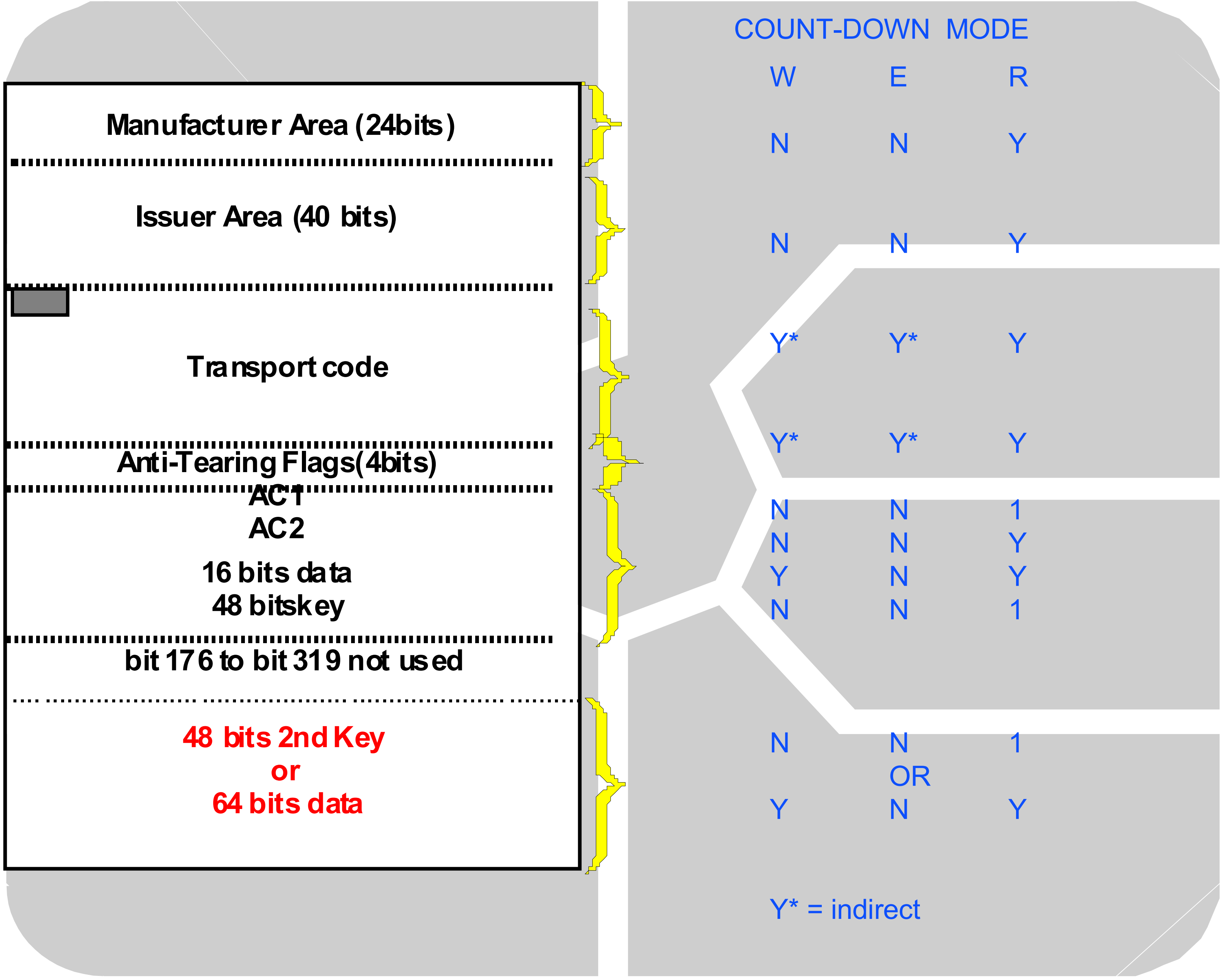






	Transport Code Presented		
	W	E	R
Manufacturer Area (24bits)	N	N	Y
Issuer Area (40 bits)	Y	N	Y
Transport code	Y	Y*	Y
Anti-Tearing Flags(4bits)	Y*	Y*	Y
AC1	N	N	1
AC2	Y	N	Y
16 bits data	Y	N	Y
48 bits key	Y	N	Y
bit 176 to bit 319 not used			
48 bits 2nd Key or 64 bits data	Y	N	Y

Y* = indirect



Manufacturer Area (24bits)

Issuer Area (40 bits)

Transport code

Anti-Tearing Flags(4bits)

AC1
AC2
16 bits data
48 bitskey

bit 176 to bit 319 not used

48 bits 2nd Key
or
64 bits data

COUNT-DOWN MODE

W	E	R
N	N	Y
N	N	Y
Y*	Y*	Y
Y*	Y*	Y
N	N	1
N	N	Y
Y	N	Y
N	N	1
N	N	1
	OR	
Y	N	Y

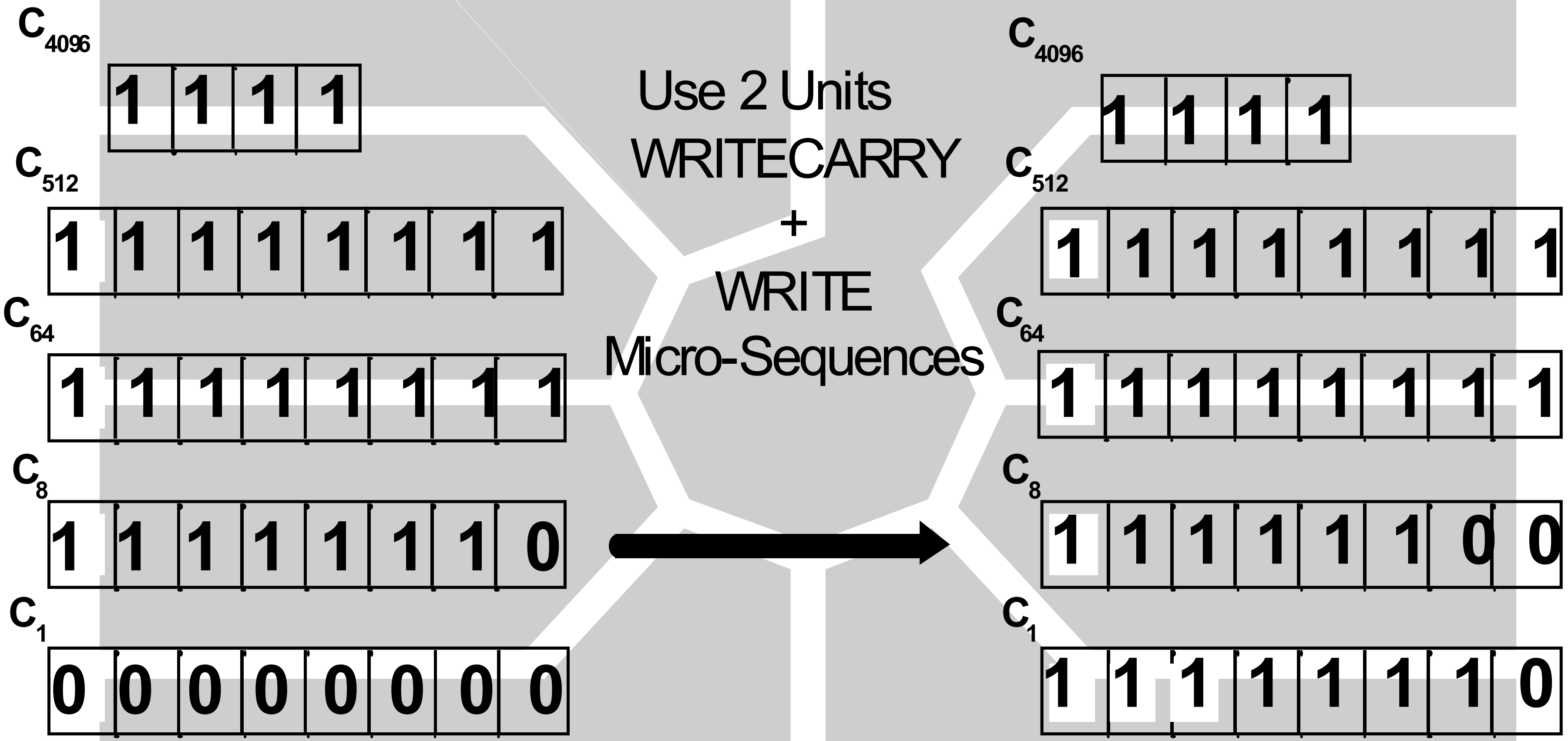
Y* = indirect

T&C Technologies

COUNT MODE

- Any unwritten counter bit can be written at any time
- **WRITE** Micro-Sequence
- Counter can be loaded with any value at personalization
- A new value can be given to counter without stepping through all intermediate values
- Counters $\mathbf{C}_1$, $\mathbf{C}_8$, $\mathbf{C}_{64}$ and $\mathbf{C}_{512}$ can be erased (refilled) by writing an unwritten bit in the next level counter
- **WRITECARRY** Micro-Sequence
- Counter $\mathbf{C}_{4096}$ cannot be erased
- Card does not propagate carries between counters
- Carry propagation must be performed by the reader with additional WRITECARRY instructions

COUNT MODE SCHEME



C_{4096} 1 1 1 1

C_{512} 1 1 1 1 1 1 1 1

C_{64} 1 1 1 1 1 1 1 1

C_{8} 1 1 1 1 1 1 1 0

C_{1} 0 0 0 0 0 0 0 0

Use 2 Units
WRITECARRY
+
WRITE
Micro-Sequences

C_{4096} 1 1 1 1

C_{512} 1 1 1 1 1 1 1 1

C_{64} 1 1 1 1 1 1 1 1

C_{8} 1 1 1 1 1 1 0 0

C_{1} 1 1 1 1 1 1 1 0

Counter status

ERASING COUNTER WITH WRITECARRY

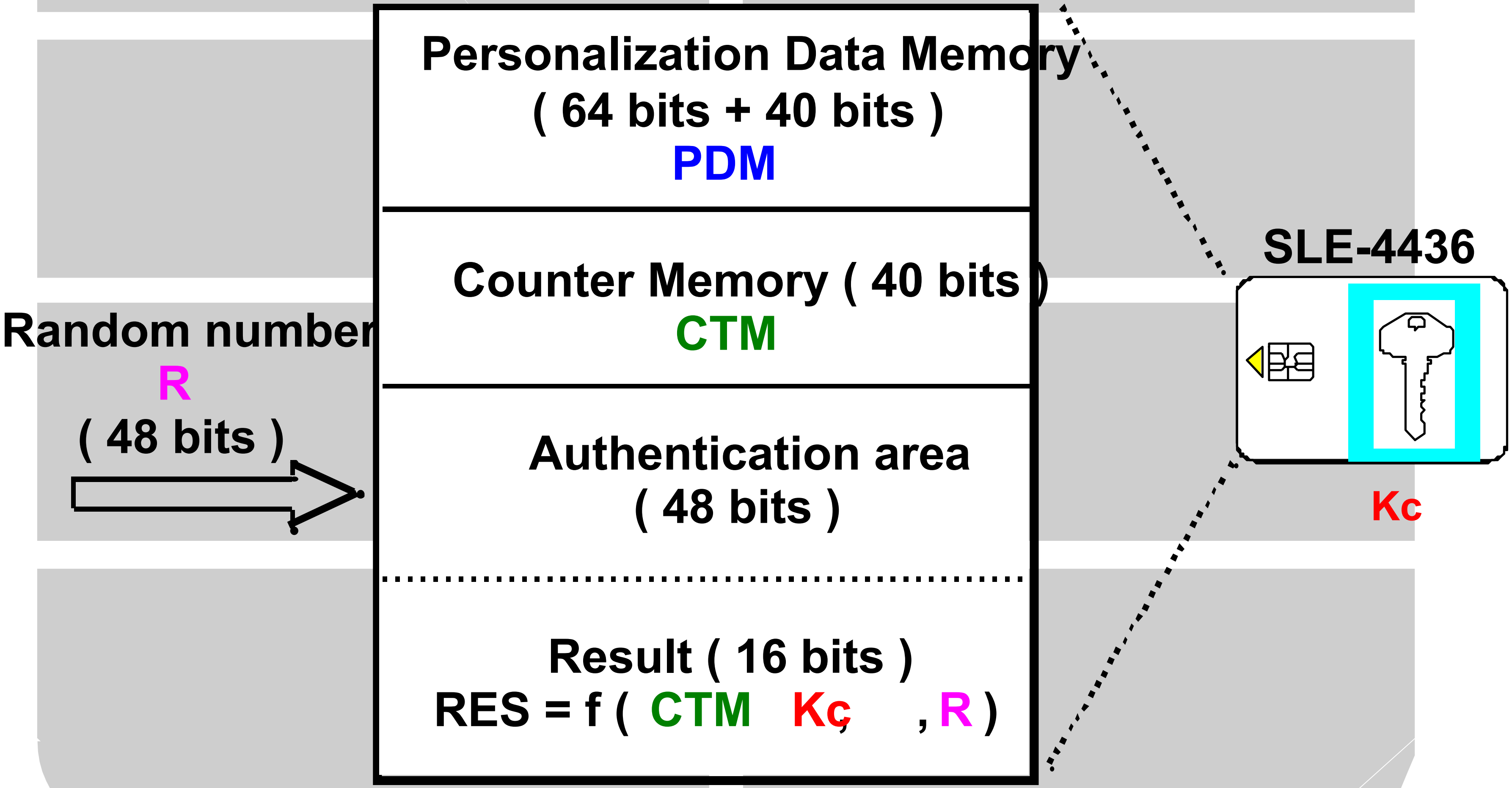
To Erase counter	WRITECARRY in
C1	C8
C8	C64
C64	C512
C512	C4096 or Logical Fuse
C4096	Impossible

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
- Protected by Transport code during delivery
- Logical security features & chip layout to avoid physical/electrical attack
- Cryptographic Card Authentication Algorithm
- SAM integrated into each application

AUTHENTICATION ALGORITHM CONCEPT



Personalization Data Memory
(64 bits + 40 bits)
PDM

Counter Memory (40 bits)
CTM

Authentication area
(48 bits)

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

Random number
R
(48 bits)

SLE-4436

Kc

T&C Technologies

CARD AUTHENTICATION SIGNALLING

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

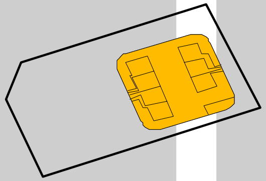
SECURITY ACCESS MODULE (SAM)

- Protection of the application key Ksam
- Calculation of the card key $Kc = f_{3DES}(PDM, Ksam)$
- Generation of the random number R
- Execution of the authentication algorithm
- Comparison of the calculated result with the result sent by the card

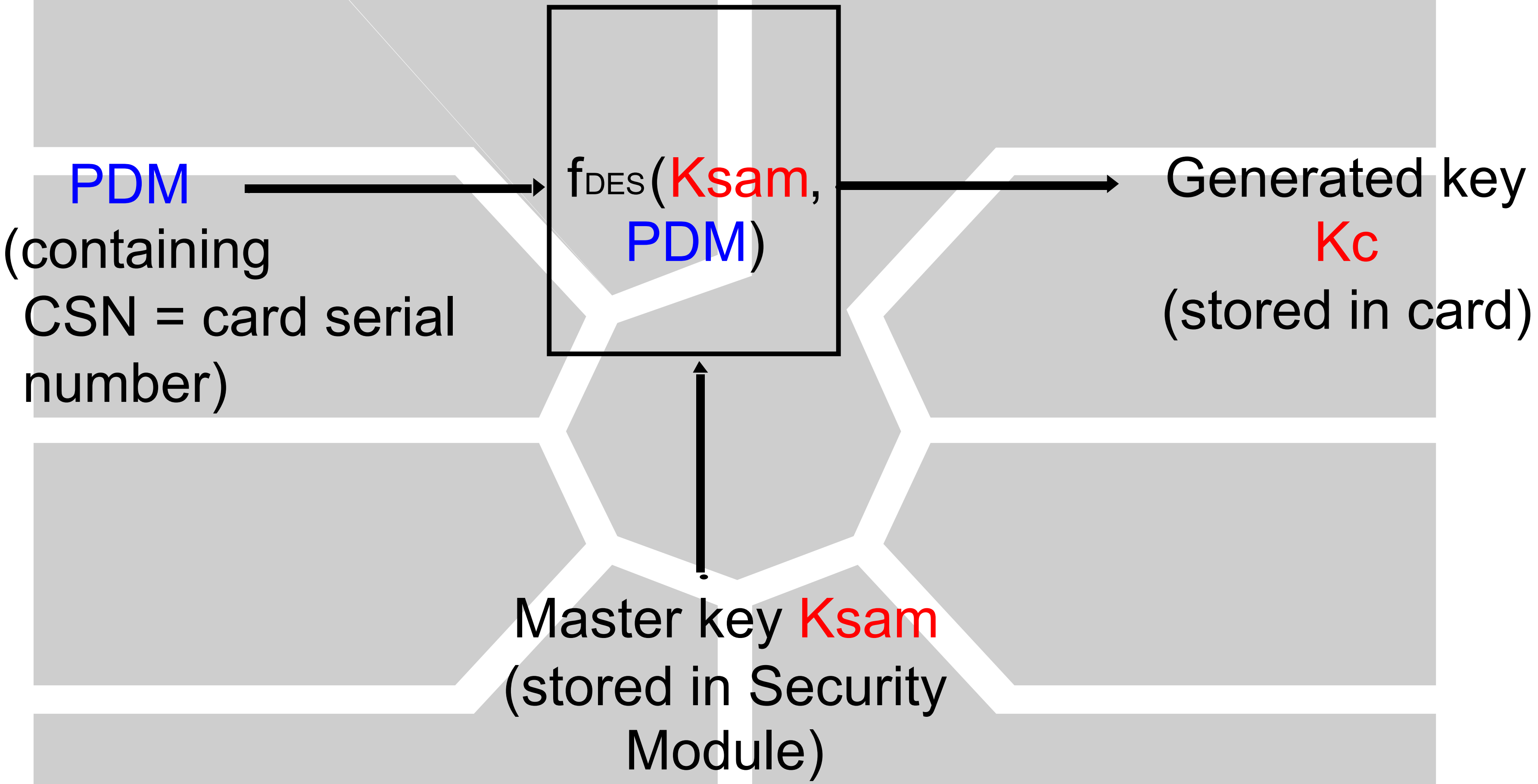
One SAM integrated into the host with one Ksam key by application

SAM CHARACTERISTICS

- ISO 7816-3 compliance
- Build 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)

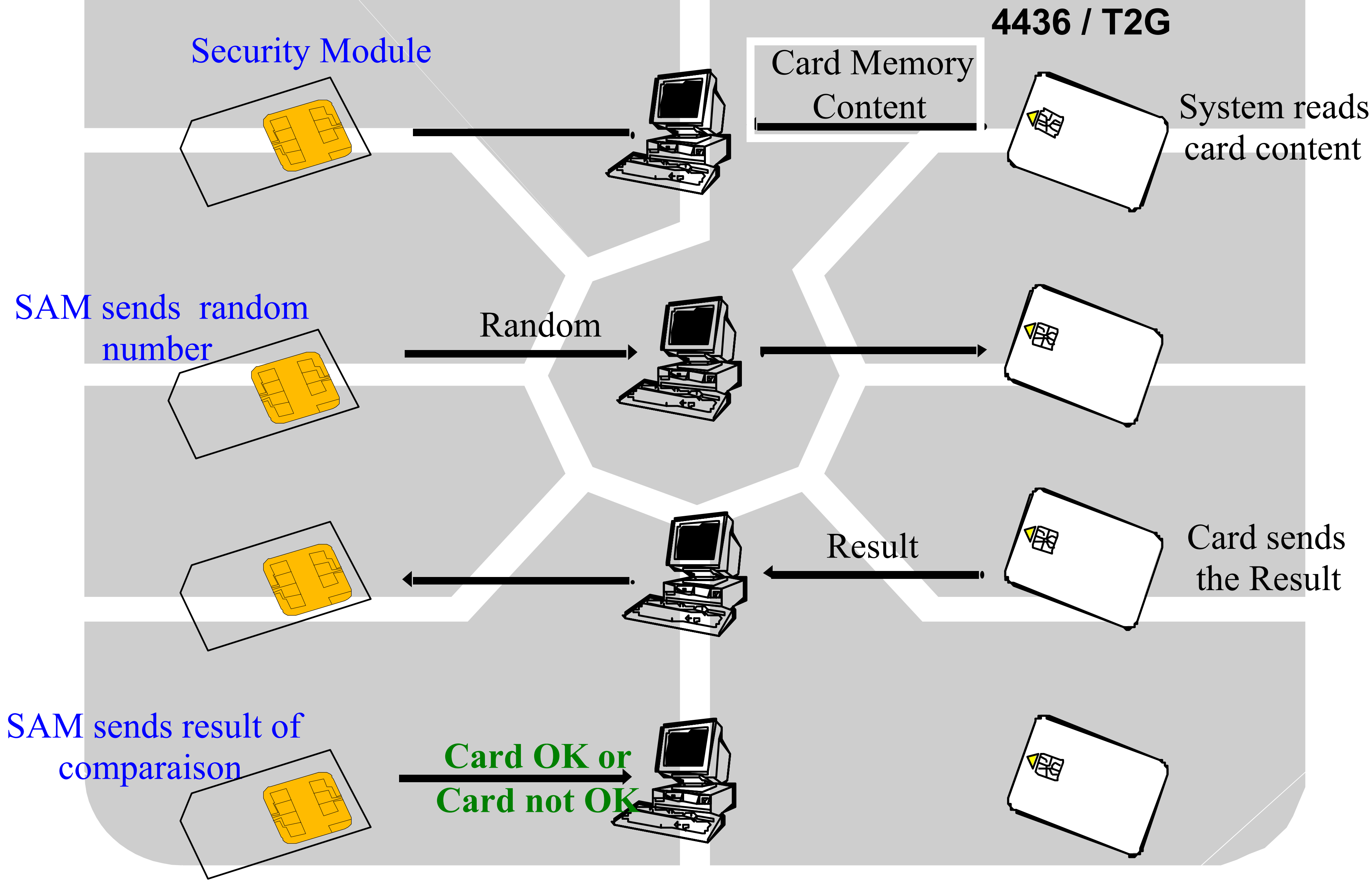
f_{DES}(Ksam, PDM)

Generated key Kc (stored in card)

Master key Ksam (stored in Security Module)

Kc always depending on a variable: the CSN

AUTHENTICATION MECHANISM



4436 / T2G

Security Module

Card Memory Content

System reads card content

SAM sends random number

Random

Result

Card sends the Result

SAM sends result of comparaison

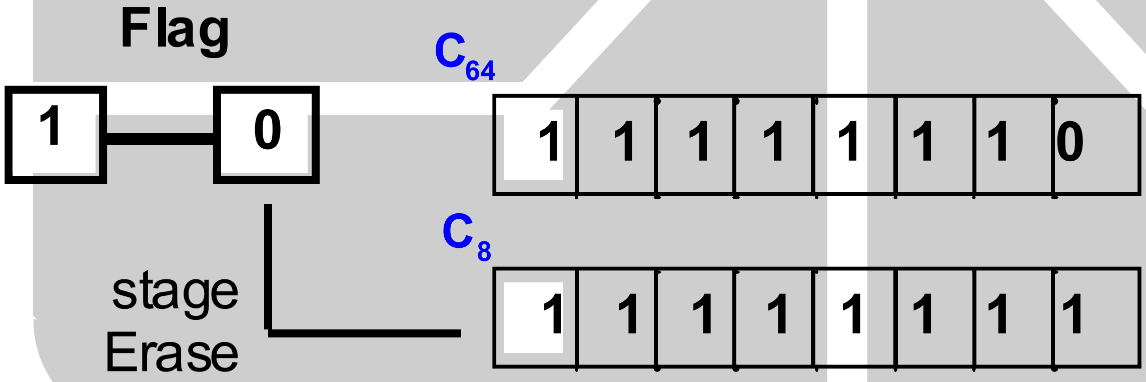
Card OK or Card not OK

ANTI PULL- OUT PROTECTION CONCEPT

- Problem :
  - Units could be lost if power goes down between writing a bit in one stage and erasing the next stage
- Solution :
  - Authorisation of erasing the next stage has to be memorised in a non-volatile way.
  - If power goes down, it will be possible after the card is power up next time, to position the counter at the previous value

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 (excepted 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 (SLE5536)

- downward compatible with SLE-4436
- ciphered block chaining of the current 16 bits response to the next authenication response computation (until the next RESET)