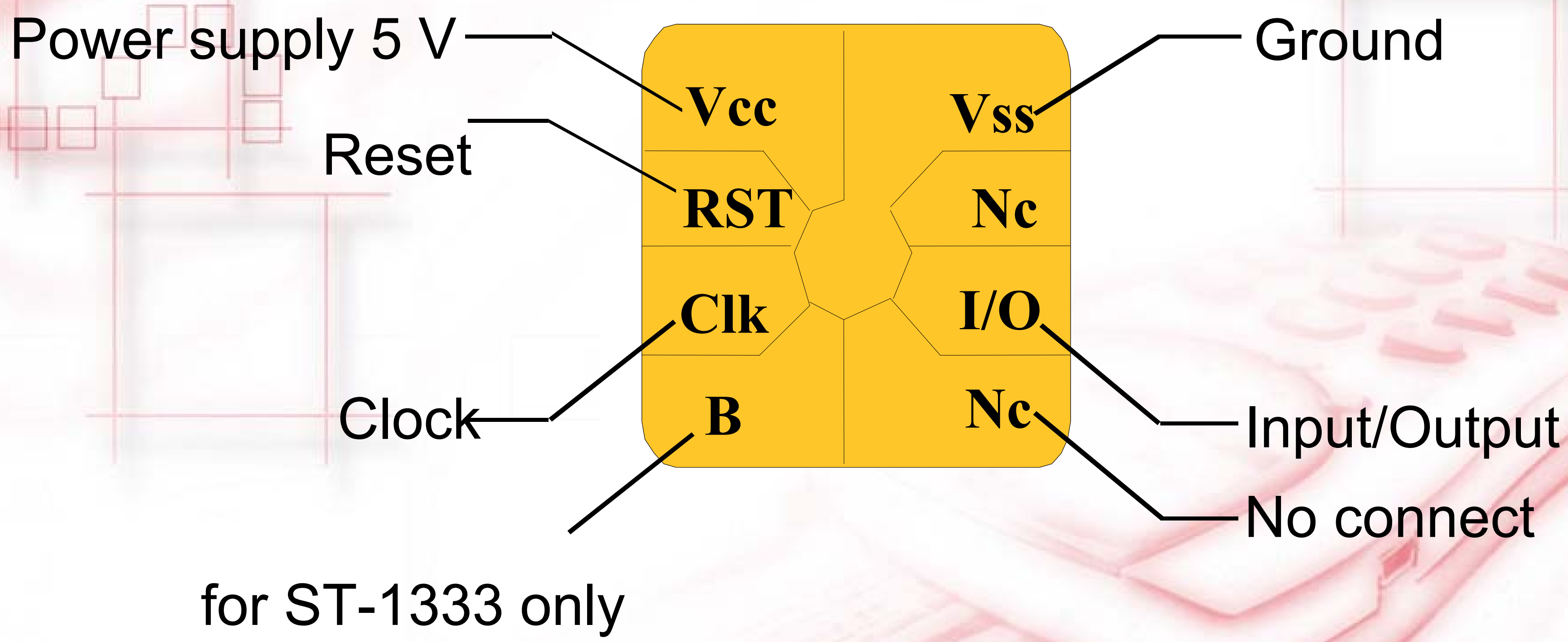
2nd Generation Telephone Card T2G (ST-1333)

- ST-1333 specifications
- Memory organization
- Card life phases
- Security features
- Card Commands

ST-1333 Specifications

- Memory divided into different areas:
  - 24 bits Manufacturer Area
  - 40 bits Issuer Area
  - 40 bits Abacus Counter Area
  - 16 bits Data Area 1 (e.g. certificate)
  - 64 bits Authentication Key Area
  - 56 bits Data Area 2
  - 32 bits anti-tearing flags
- Counter capacity of up to 32768
- Pull out protection
- Active card authentication

PIN Assignments

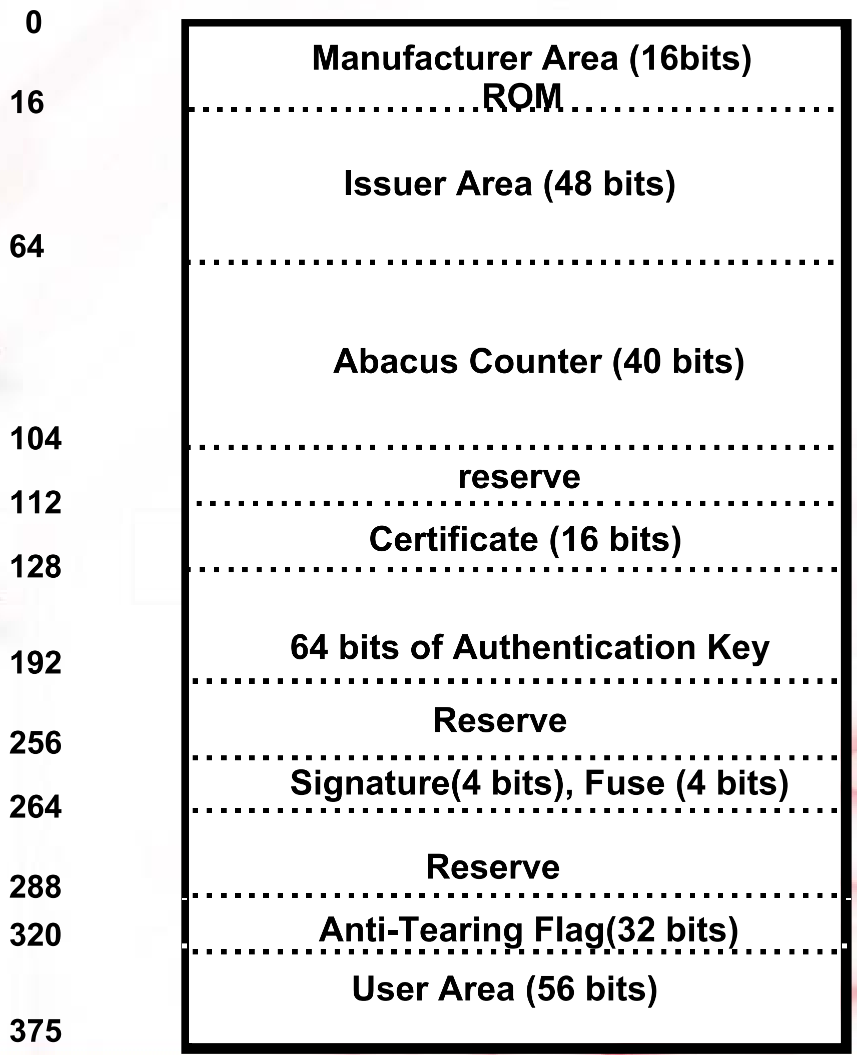


ISO 7816-1 / -2 compatible

Electrical Characteristics

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

Memory Organization



0

Manufacturer Area (16bits)
ROM

16

Issuer Area (48 bits)

64

Abacus Counter (40 bits)

104

reserve

112

Certificate (16 bits)

128

64 bits of Authentication Key

192

Reserve

256

Signature(4 bits), Fuse (4 bits)

264

Reserve

288

Anti-Tearing Flag(32 bits)

320

User Area (56 bits)

375

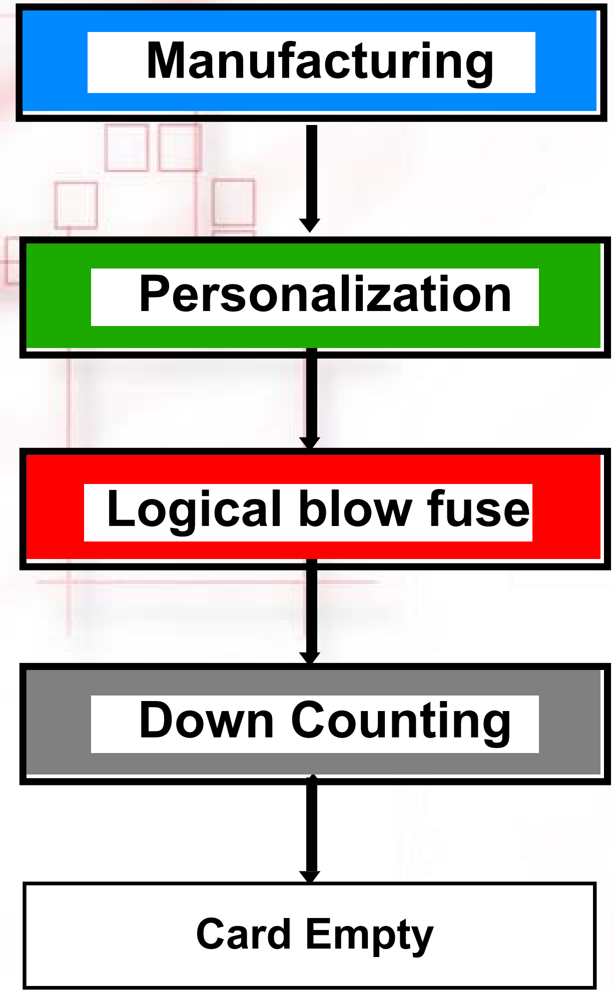
Additional Features Compared to the SLE-4406

- Card cryptographic authentication algorithm
- More memory, a 72 bits extended Issuer Area
- a 64 bits Authentication Key
- 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



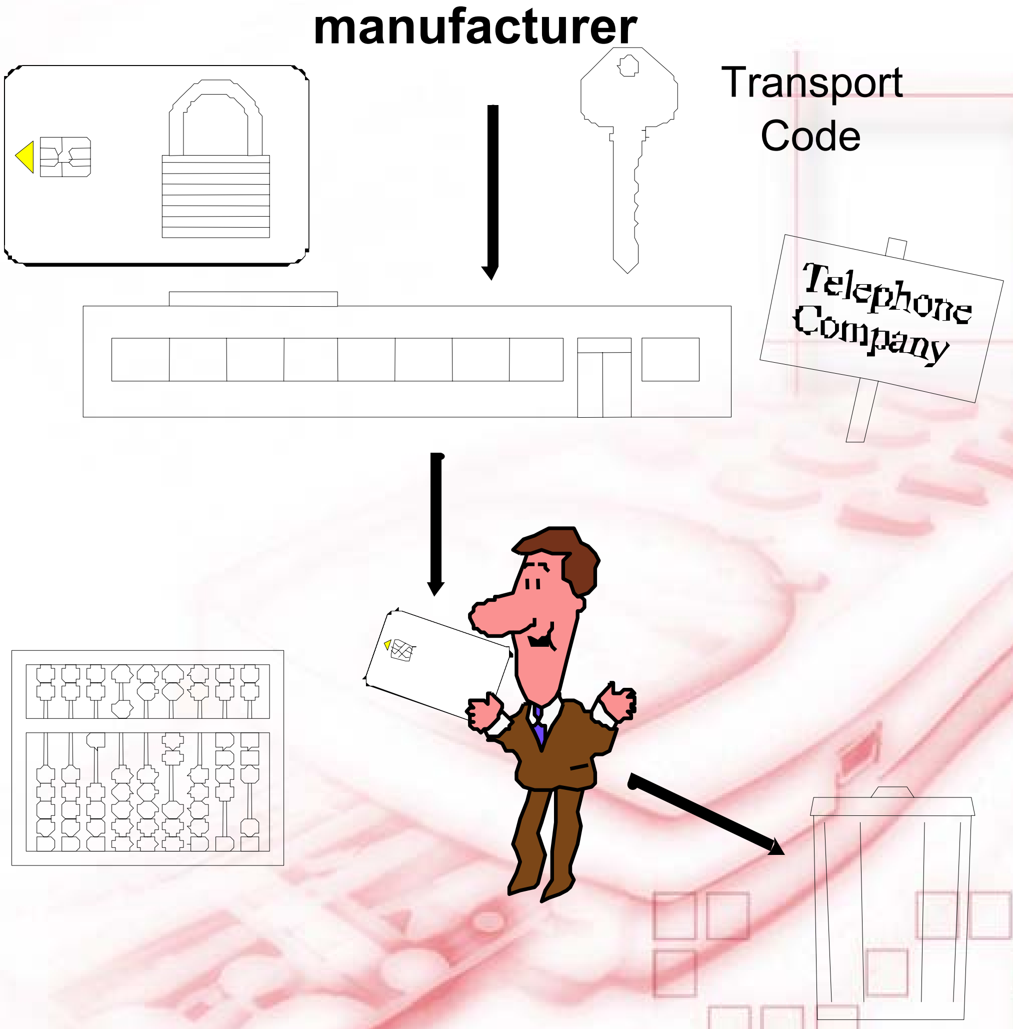
Manufacturing

Personalization

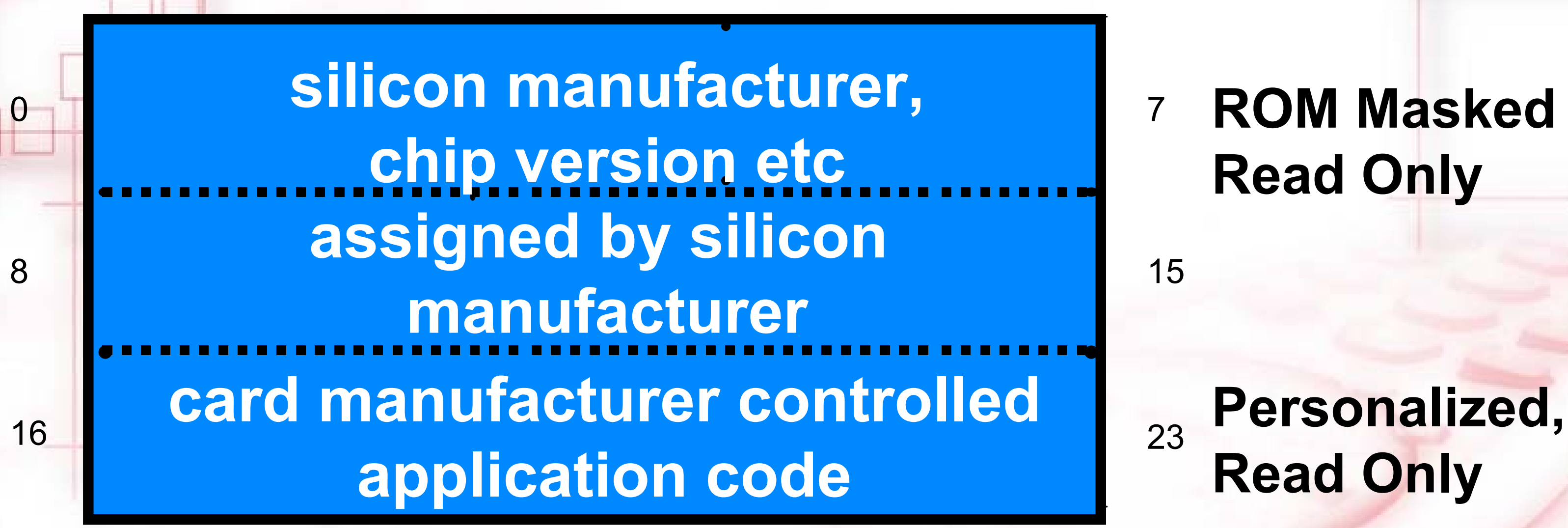
Logical blow fuse

Down Counting

Card Empty



Manufacturer Area


0
silicon manufacturer, chip version etc
7
ROM Masked
Read Only
8
assigned by silicon manufacturer
15
16
card manufacturer controlled application code
23
Personalized,
Read Only

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

Personalization

- Present transport code
- Write Issuer Area, Ki
- Clear counters
- Blow logical fuse
- Set initial value

T2G Issuer Mode Memory Access

	Area	Read	Write	Erase
0-1	Chip ID	Y	N	N
2-7	Card ID	Y	Y if CODE	N
8	Counter 6	Y	Y	N
9	Counter 5	Y	Y	N
A	Counter 4	Y	Y	N
B	Counter 3	Y	Y	N
C	Counter 2	Y	Y	N
D	Not Used			
E-F	Certificate	Y	Y	N
10-17	Ki	Y	Y if CODE	N
18				
20	**Signature**	Y	N	N
20	**Fuse**	Y	Y if CODE	N
21-23	Not Used			
24	Anti-Tearing Flag5	Y	N	N
25	Anti-Tearing Flag4	Y	Y write C5	N
26	Anti-Tearing Flag3	Y	N	N
27	Anti-Tearing Flag2	Y	N	N
28-2E	User Area	Y	Y	Y/N option

T2G User Mode Memory Access

Addr	Area	Read	Write	Erase
0-1	Chip ID	Y	N	N
2-7	Card ID	Y	N	N
8	Counter 6	Y	Y	N
9	Counter 5	Y	Y	Y,C6
A	Counter 4	Y	Y	Y,C5
B	Counter 3	Y	Y	Y,C4
C	Counter 2	Y	Y	Y,C3
D	Not Used			
E-F	Certificate	Y	Y	N
10-17	Ki	Y	Y	N
18				
20	Signature	Y	N	N
20	Fuse	Y	Y	N
21-23	Not Used			
24	Anti-Tearing Flag5	Y	Y,write C6	Y,erase C5
25	Anti-Tearing Flag4	Y	Y,write C5	Y,erase C4
26	Anti-Tearing Flag3	Y	Y,write C4	Y,erase C3
27	Anti-Tearing Flag2	Y	Y,write C3	Y,erase C2
28-2E	User Area	Y	Y	Y/N options

Fuse Blow

Byte 33

		select test fuse	test fuses A & B	select issuer fuse	issuer fuses A&B
	bit	260	261	262	263

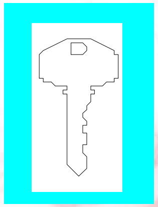
- PROG at select bit toggles A,B
- test+issuer fuse B blown to test blowing+sensing circuit at chip factory
- test fuse A blown at chip factory
- issuer fuse B blown at card factory after initializations
- reading & writing access is free in TEST and USER mode, writing TSC=1 at card factory,reading is free

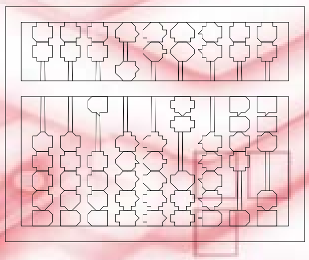
Before and After Fuse Blow

- Before (Personalization Mode)
  - 16-bits manufacturing information (read only)
  - Protected by transport code
  - 8 attempts to present transport code then the card is useless
  - Loadable counter with value 0-32768
- After (Count Down Mode)
  - Down counter from loaded value to zero
  - Issuer and manufacturer information is read only
  - No access to key area after the fuse blown
  - Extended data area READ / WRITE /ERASE

Count Down Phase

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





Count Mode

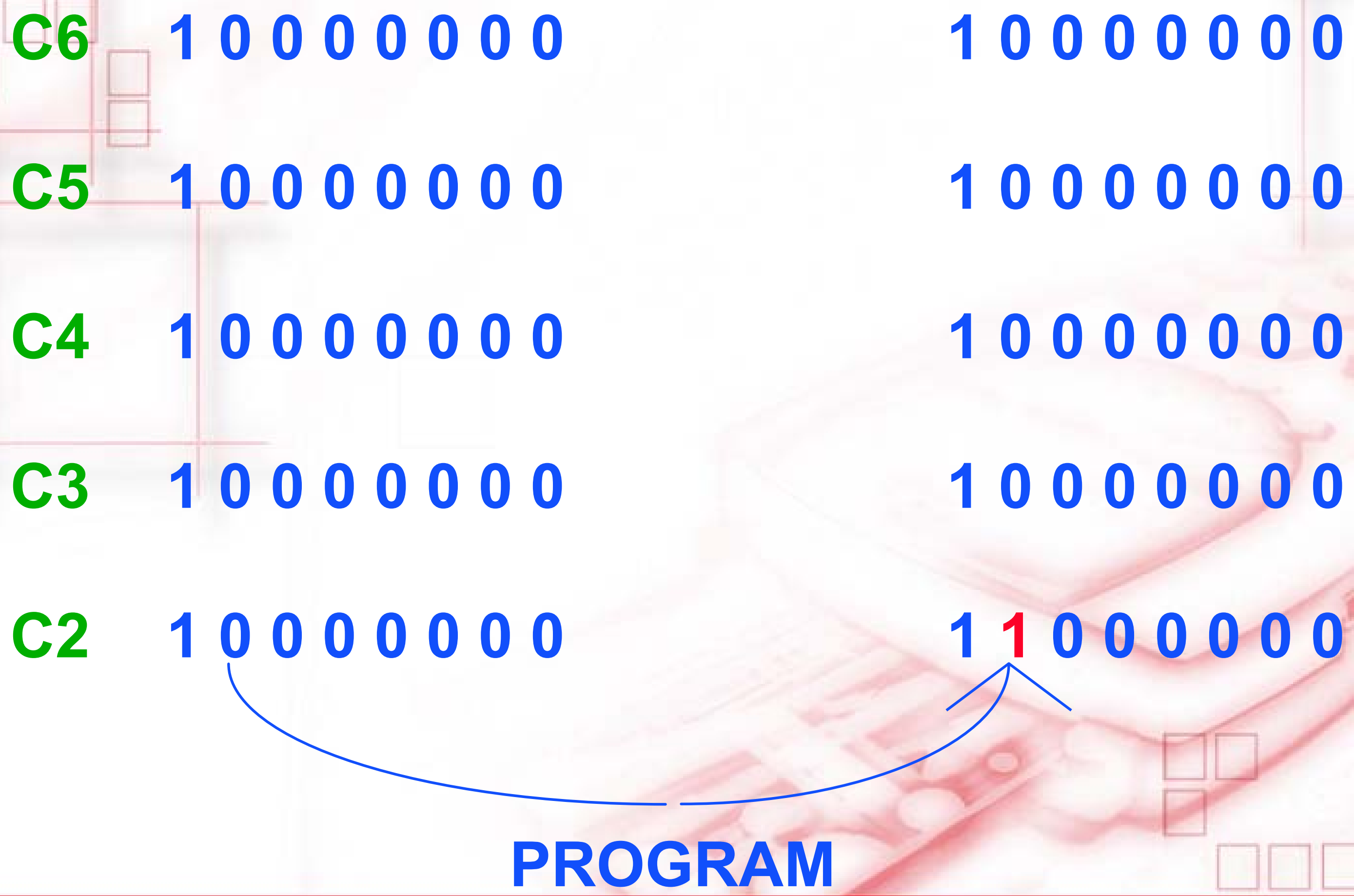
- Any unwritten counter bit can be written at any time
- **PROGRAM** Micro-Sequence
- Counter can be loaded with any value at personalization
- A new value can be given to counter without stepping through all intermediate values
- Counters C3, C4, C5 & C6 can be erased (refilled) by writing an unwritten bit in the next level counter
- **PROGRAM (FOR ERASE)** Micro-Sequence
- Counter **C6** cannot be erased
- Card does not propagate carries between counters
- Carry propagation must be performed by the reader with additional PROGRAM (FOR ERASE) instructions

Erasing Counter With WRITECARRY

To erase counter	PROGRAM (for ERASE) in
C2	C3
C3	C4
C4	C5
C5	C6
C6	Impossible

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

T2G Count Down Scheme



C6	1 0 0 0 0 0 0 0	1 0 0 0 0 0 0 0
C5	1 0 0 0 0 0 0 0	1 0 0 0 0 0 0 0
C4	1 0 0 0 0 0 0 0	1 0 0 0 0 0 0 0
C3	1 0 0 0 0 0 0 0	1 0 0 0 0 0 0 0
C2	1 0 0 0 0 0 0 0	1 1 0 0 0 0 0 0

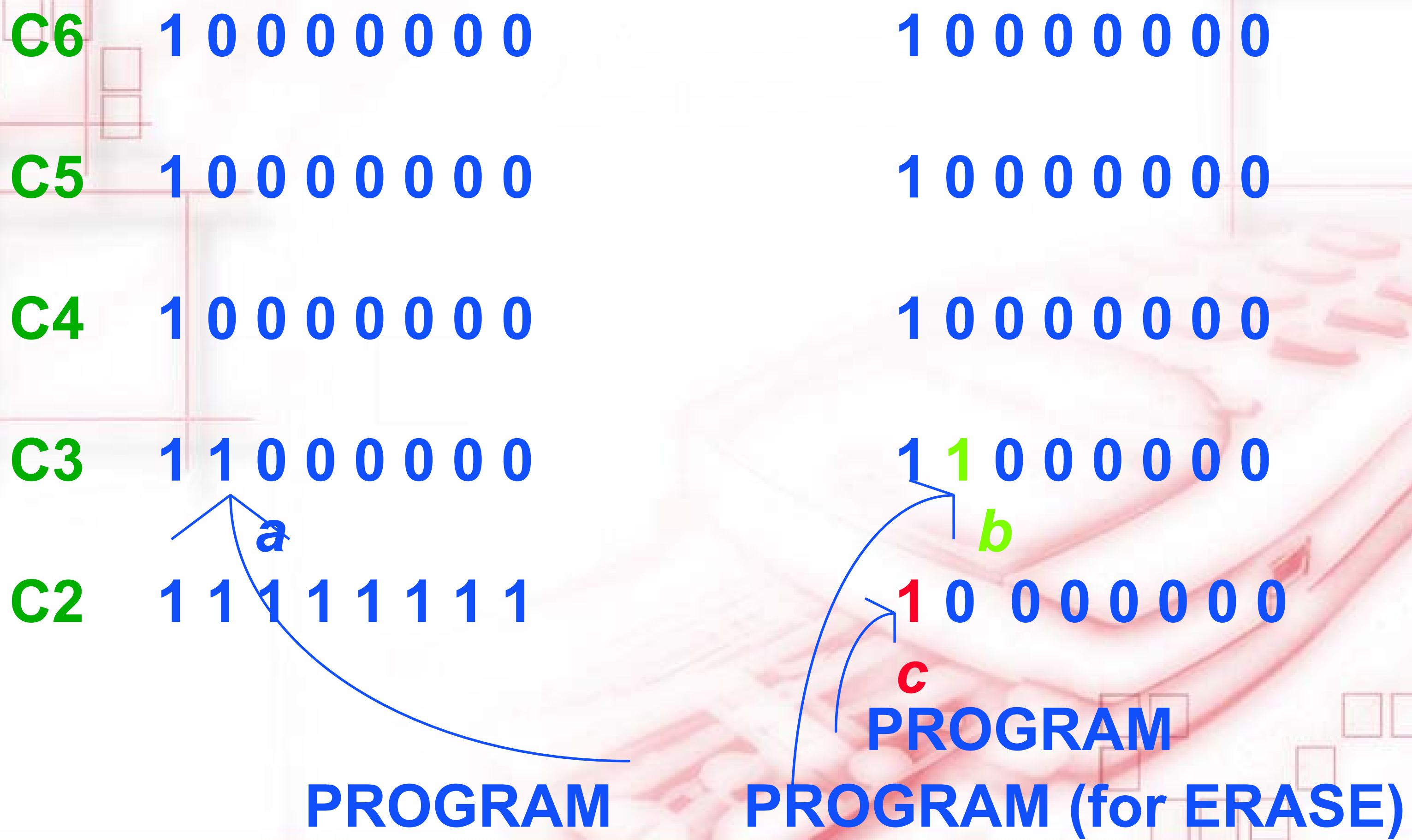
PROGRAM

T2G Count Down Scheme

C6	1 0 0 0 0 0 0 0	1 0 0 0 0 0 0 0
C5	1 0 0 0 0 0 0 0	1 0 0 0 0 0 0 0
C4	1 0 0 0 0 0 0 0	1 0 0 0 0 0 0 0
C3	1 0 0 0 0 0 0 0	1 0 0 0 0 0 0 0
C2	1 0 0 0 0 0 0 0	1 1 1 1 1 1 1 1

PROGRAM

T2G Count Down Scheme



C6	1 0 0 0 0 0 0 0	1 0 0 0 0 0 0 0
C5	1 0 0 0 0 0 0 0	1 0 0 0 0 0 0 0
C4	1 0 0 0 0 0 0 0	1 0 0 0 0 0 0 0
C3	1 1 0 0 0 0 0 0	1 1 0 0 0 0 0 0
C2	1 1 1 1 1 1 1 1	1 0 0 0 0 0 0 0

PROGRAM

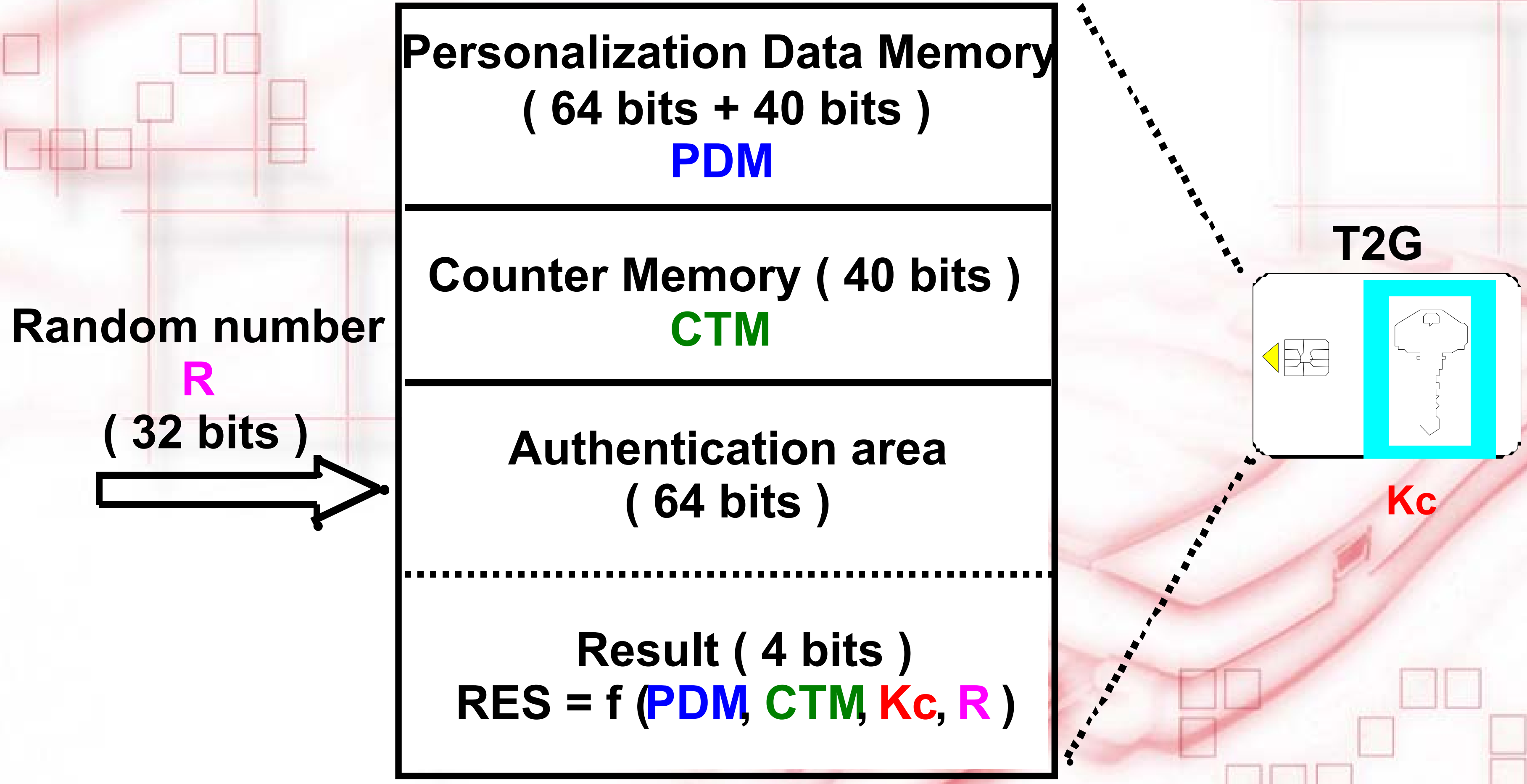
PROGRAM

PROGRAM (for ERASE)

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
(64 bits)

Result (4 bits)
RES = f (PDM, CTM, Kc, R)

Random number
R
(32 bits)

Card Authentication Signaling

- RESET
- 260 X READ
- RESET
- For i=0 to 31
  - if random number = 1, PROG
  - READ
- 227 X READ
- RESET
- 255 X READ
- 4 X READ to read signature bit 0,1,2,3

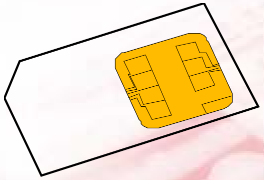
Security Access Module (SAM)

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

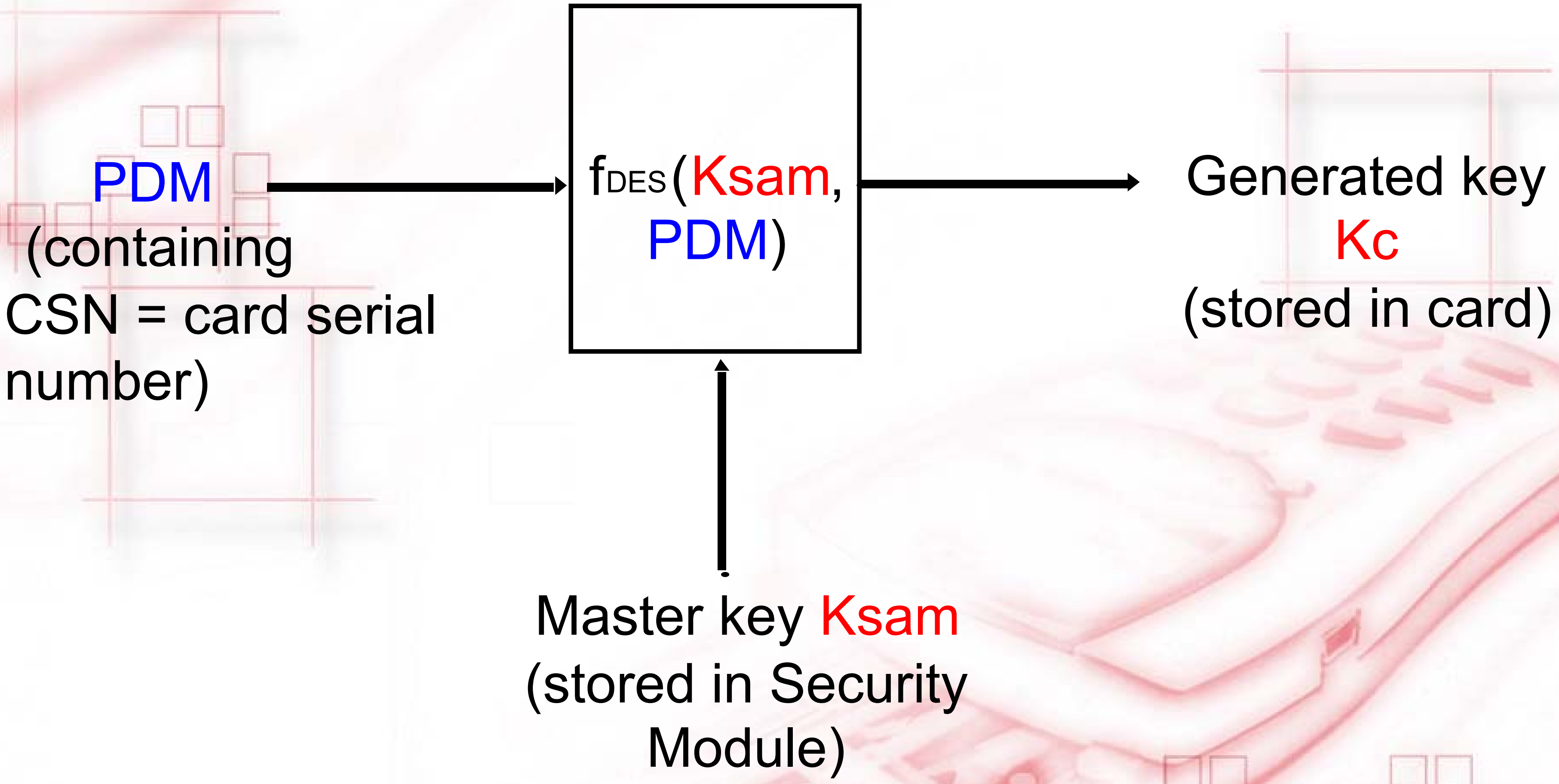
One SAM integrated into the host with one Ksam key by application

SAM Characteristics

- ISO 7816-3 compliance
- Build on top of a CPU smart card
- Command set 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)

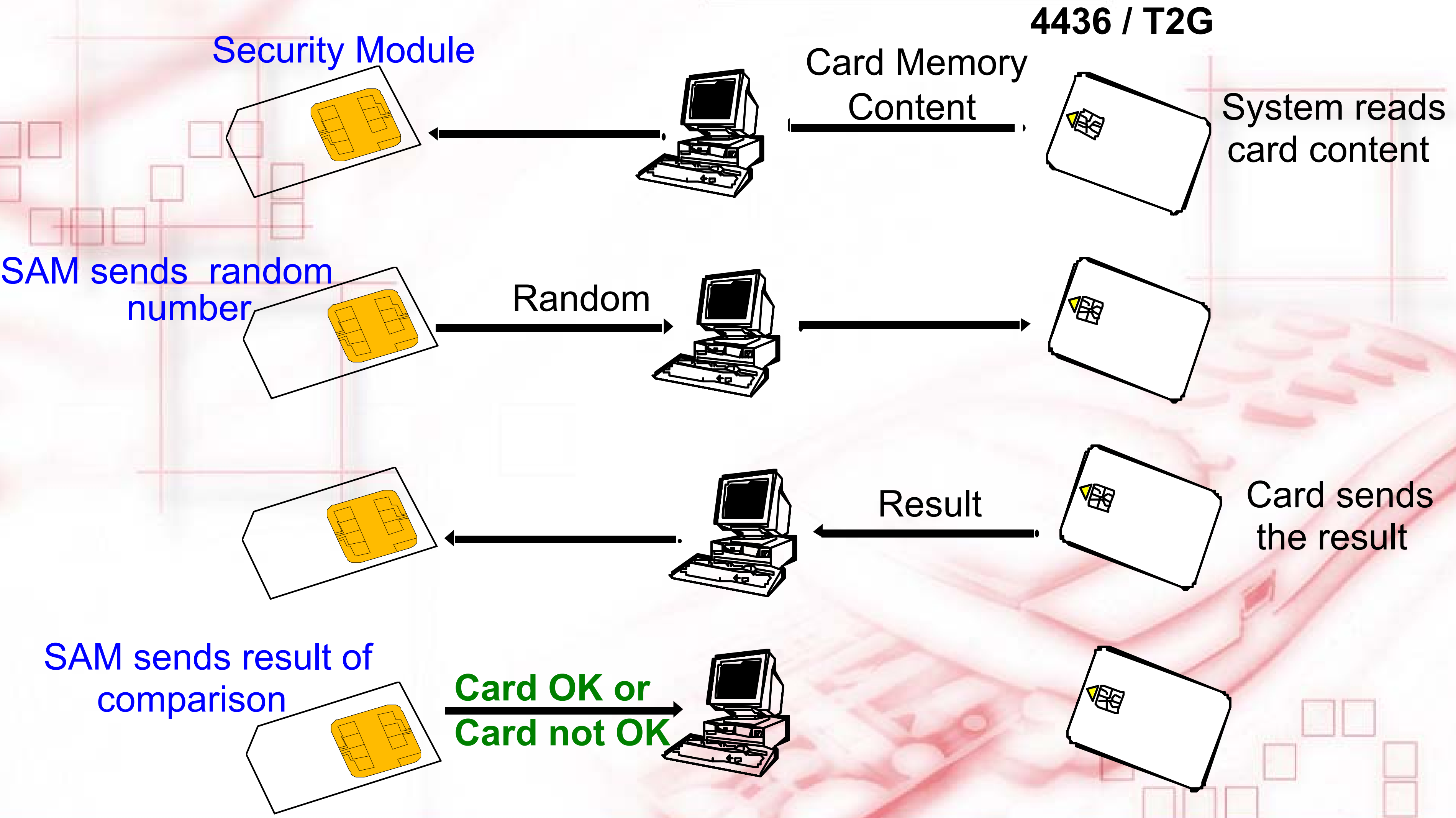
f_{DES}(Ksam, PDM)

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 comparison

Card OK or Card not OK

Anti-Pull Out Protection Mechanism

- Problem:
  - Units could be lost if power goes down between writing a bit in one stage and erasing 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 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 "0" to "1" before erasing the lower stage counter

Card Commands

- Reset Address Counter (RESET)
- Increment Address Counter and Read Bit (READ)
- Write Bit (PROGRAM)
- Compare(COMPARE)
- Write Carry and Erase Counter Stage (2 PROGRAM commands)
- Authentication (combination of READ & PROGRAM)