

Automatic Teller Machine



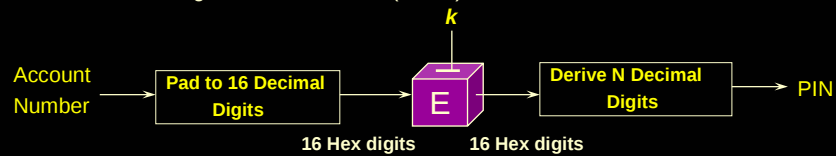
Security Problems with ATM

-
-

Personal Identification Number

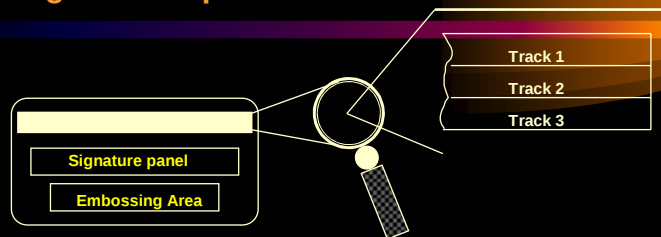
- Customer-SELECTED PIN
- Assigned Random PIN
- Assigned Derived PIN (offline)

8807012345691715
 FEFEEEEEEEEEEFE
 A2CE126C69AEC82D
 0224126269042823
 0224



Automatic Teller Machine

Magnetic Stripe Card

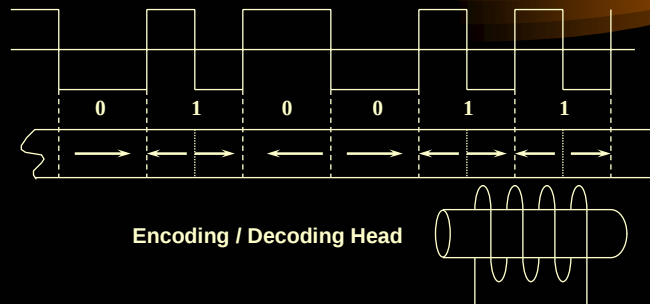


- **Track 1** : International Air Transportation Association (IATA)
 - airline ticketing applications, 29 alphanumeric characters
- **Track 2** : American Bankers Association (ABA)
 - on-line financial transactions, 40 numeric characters
- **Track 3** : Financial Transactions
 - financial transactions, 107 numeric digits

Automatic Teller Machine

❑ Magnetic Stripe Card

❑ Encoding / Decoding



- **flux reversal** for each pair of contiguous bits
- a single domain for '0'
- two domains for '1'

Automatic Teller Machine

❑ Magnetic Stripe Card

❑ Magnetic Stripe Security

- (Theft)
- (Counterfeit)
- Buffering : , (offline)
- Skimming : , (offline)

❑ Card Standard

- ISO 7810, 7811 : physical dimension of card
- ISO 7812, 7813 : logical structure of card
- ISO 7816 : smartcard

Automatic Teller Machine

❑ ATM Fraud

❑ Outsider Attack

- < case 1 > PIN + ATM Ticket → Card
- < case 2 > ATM
- < case 3 >
- < case 4 > ATM

❑ Insider Attack

- < case 1 >
- < case 2 > ATM ATM



Automatic Teller Machine

❑ On-Line and Off-Line Operation



Bank's Central DB

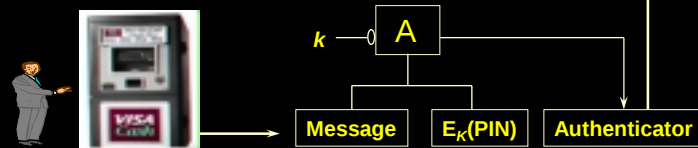
- How to do PIN checking
 - Off-line : A/C Number → PIN
 - On-line : Bank's central Database
- Transaction checking
- forged Card
- Blacklist

Automatic Teller Machine

Transaction between ATM and Host

Request from ATM to Host

- ATM Identity
- Account Number
- PIN encrypted
- Amount of Cash requested
- Sequence Number of Transaction
- Authenticator for all the other data



Automatic Teller Machine

Transaction between ATM and Host

Response from Host to ATM

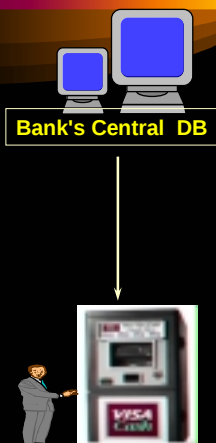
- ATM Identity
- Operation Code (Approval or Denial)
- Sequence Number of Transaction
- Authenticator for all the other data

Sequence Number of Transaction

- Protection against Replay Attack

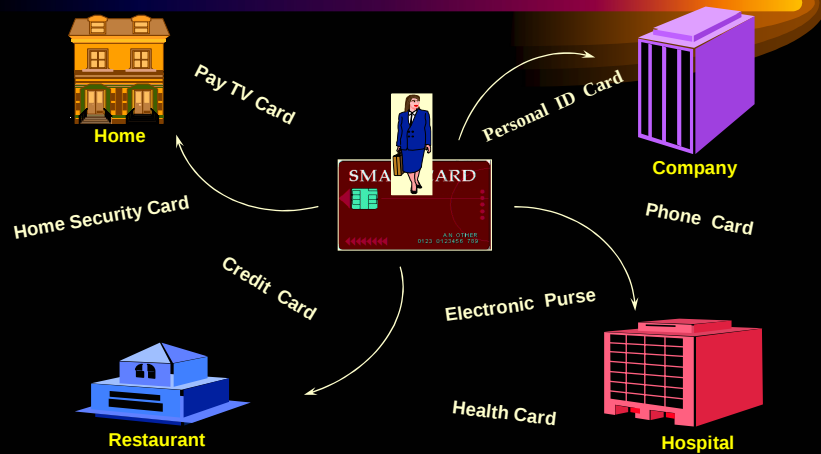
A Log at ATM

- Response Message may not get through



SMARTCARD

❑ Smartcard and Life



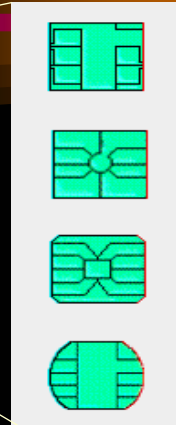
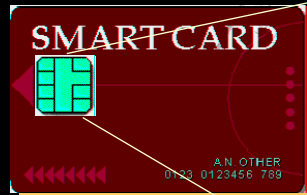
SMARTCARD

❑ Cryptography in Smartcard

- ❑ Data Encryption Standard (DES)
- ❑ Access Control
- ❑ Message Confidentiality
- ❑ Message Integrity and Authentication
- ❑ Sender Authentication
- ❑ Rivest-Shamir-Adleman (RSA)
- ❑ Digital Signature

SMARTCARD

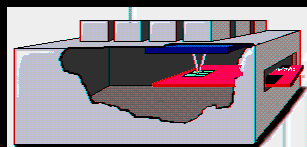
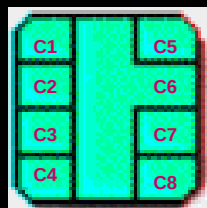
□ Smartcard Contact Pad



- Contact Pads looks different
- ISO 7816-1 ~ 6
- Means by which Card Reader makes electrical contact with the card

SMARTCARD

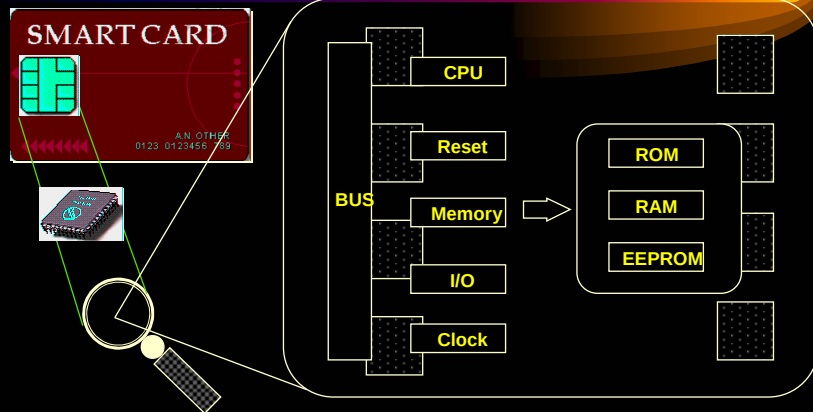
□ Smartcard Contact Pad



- C1 : power supply input (Vcc)
- C2 : RST for reset signal to card
- C3 : CLK (clock)
- C4 : not defined
- C5 : GND (ground)
- C6 : Vpp
- C7 : communication
- C8 : not defined

SMARTCARD

❑ Smartcard



SMARTCARD

❑ Smartcard CPU and Operating System

❑ Smartcard CPU

- INTEL 8051, Motorola 6805 8-bit processor
- 32-bit processor based on RISC architecture

❑ Smartcard Chip Category

- Dumb Cards, Wired Logic Cards
- Smartcards

❑ Smartcard Operating System

- OS controls card
- commands to open, read, write, erase files
- access control to files through key or PIN
- message certification, and communication

SMARTCARD

Smartcard Memory

Volatile Memory

- DRAM
- Scratchpad, RAM Stack (Working Area)
- 128 ~ 512 Bytes

Nonvolatile Memory

- ROM
 - Smartcard Operating System, Card Mask
 - 2 ~ 16K Bytes
- EEPROM, Flash Memory
 - User/Application Area (UAM)
 - 1 ~ 16 K Bytes



SMARTCARD

Smartcard Chip Manufacturer

Chip	Maker	Core	RAM (bytes)	ROM (Kbytes)	NVM (Kbytes)	Surface (mm)
SC01	Motorolla	68HC05	36	1.6	1	3.5 x 5.5
SC24	Motorolla	68HC05	128	3	1	4.14 x 3.44
SC28	Motorolla	68HC05	240	12.8	8	27
ST1821	Thompson	8048	44	2	1	3.4 x 5.36
ST16301	Thompson	68HC05	160	3	1	3.66 x 4.93
ST16F48	Thompson	68HC05	512	16	8	4.8 x 4.9
44C10	Siemens	80C51	128	4	1	13
44C40	Siemens	80C51	256	8	4	18.39
44C80	Siemens	80C51	256	16	4	24.49

SMARTCARD

❑ Smartcard Chip with Coprocessor

- Public-Key Cryptosystem
- 8-bit Processor and Coprocessor for modular exponentiation
- ISO 7816-1, chip size of 25mm², some EEPROM area occupied

Name	Maker	Core	Core	ACP	RAM	EE	ROM
ST16CF54	Thompson	68HC05	secret	secret	352	16	16
ST16KL74	Thompson	68HC05	secret	secret	608	20	20
SLE44C200	Siemens	80C51	24.5	5.7	256	9	9
SLE44CR80S	Siemens	80C51	<25		256	8	17
P83C852	Philips	80C51	22.3	2.5	256	2	6
P83C858	Philips	80C51			640	8	20
MC68HC05	Motorolla	68HC05	27	5	512	4	13.3
CY512i	Cylink	80C31	73		768	8	8

SMARTCARD

❑ Other Circuits

❑ RST and ATR

- RESET signal, card initialization
- Answer to RESET signal, (card type and application type)

❑ Synchronization Circuit

- Timing signal from internal clock or external clock
- synchronize card's internal operations and communications
- 5 ~ 14 MHz

❑ Communication Circuit

- I/O Port in contact C7
- Synchronous or Asynchronous Mode
- Internal Amplifier

SMARTCARD

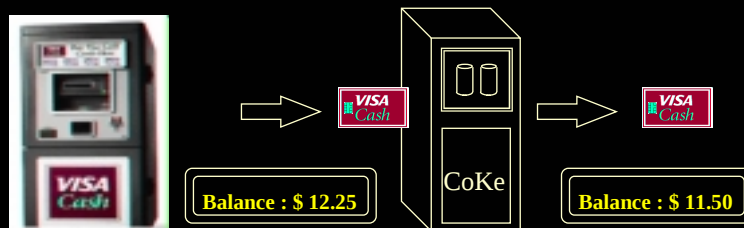
□ Financial Applications

- **Smartcard and Bank**
 - price, **off-line transaction**, magnetic stripe card
- **Prepaid Cards**
 - substitution for cash, off-line transaction
 - U.S. **VISA Cash**, electronic purse system
- **Banking Cards**
 - France (1991), Smart Bank Card based on **BULL CP8**
 - Norway, the problem of high communication costs due to on-line
- **Super Smartcard**
 - smartcard with keyboard and display, 0.76mm thick
 - **Untraceability**

SMARTCARD

□ VISA Cash

- **Small-Amount Transactions**
 - Convenience Store
 - Vending Machine
 - Restaurant



SMARTCARD

❑ Medical Applications

❑ Health Care Cards

- Identification
- Health Payments
- Communications
- Health records
- Information



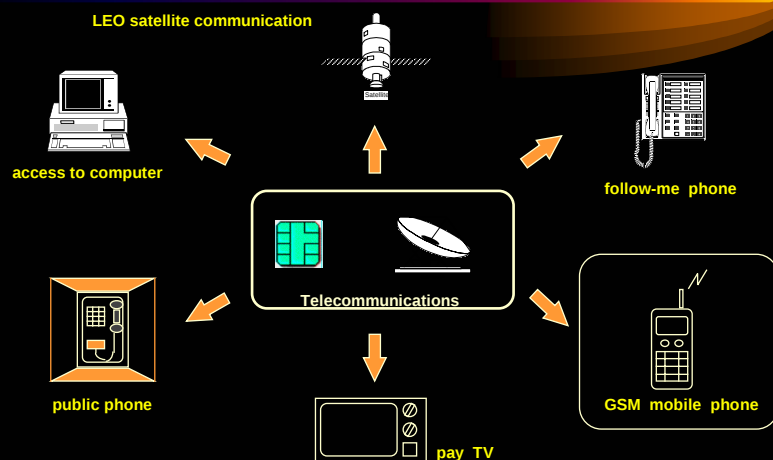
❑ Optical Cards and Smartcards

❑ U.K Health Care Project

- 2K BULL CP8 Smartcard
- 5-character alphanumeric coding of pathologies
- International Classification of Diseases

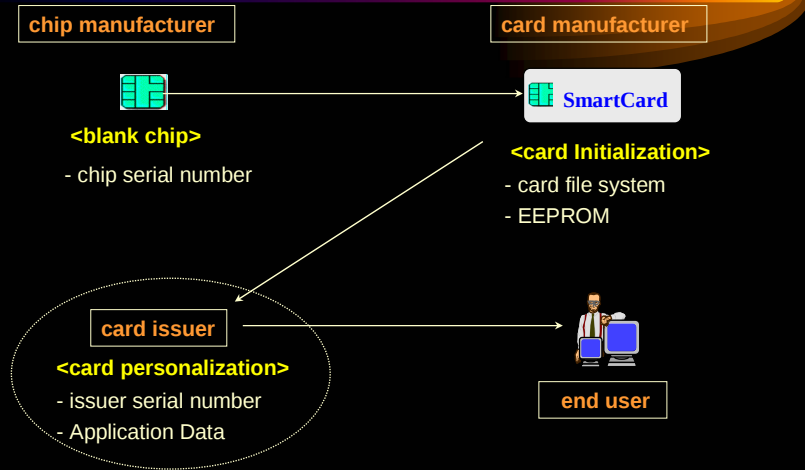
SMARTCARD

❑ Telecommunication and Computer Cards



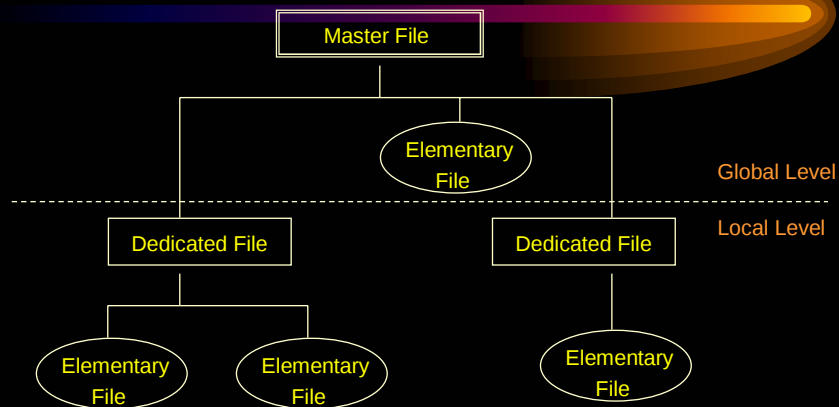
SMARTCARD

❑ GPK2000 Card Life Cycle



SMARTCARD

❑ GPK2000 File System



SMARTCARD

□ GPK2000 File Descriptor

2-byte		2-byte	
File Pedigree	File Number	File Identifier	
FDB	OPT(00)	Body Size	
	Group 1 AC	Group 2 AC	
	Group 3 AC	Status(00)	Checksum

0 0 x x x 0 0 0

- 1 1 1 Dedicated File
- 1 0 1 Key Elementary File (EFkey)
- 1 0 0 Secret Code Elementary File (EFsc)
- 0 1 1 Purse Elementary File
- 0 1 0 Transaction Manager Elementary File
- 0 0 0 All other Elementary File

File Descriptor

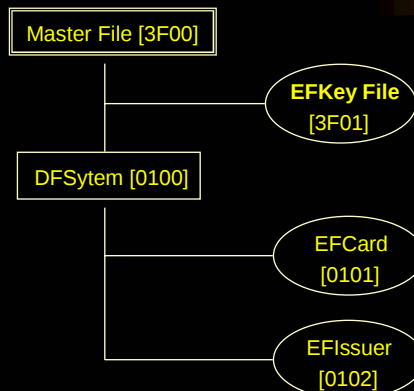
File Body

SMARTCARD

□ GPK2000 Initial File Structure

- Master File, Dedicated File (up to 63 EFs), Elementary File

→ directory for application



SMARTCARD

□ Key File (EFkey)

- 1 or more Key Files for Master or Dedicated File
- Up to 8 Keys for each EFkey
- Cryptographic Key : 12-byte
- **Type** : Administration Key Payment Key
session-key , authentication, secure messaging
- **Kv** : Key Version (default to 0)
- **Cks** : checksum, XOR on 11 bytes and inverting result
- **K1~8** : key values (64-bit)

Type	00	Kv	Cks
K8	K7	K6	K5
K4	K3	K2	K1

Key File

SMARTCARD

□ Secret Code File (EFsc)

- Up to 1 Secret Code File for Master or Dedicated File
- Up to 8 Secret Codes for each EFsc
- 8-byte for a secret code

Mode	MPN	00	SCR	00	UCR	00	00
Secret Code (4-byte)							

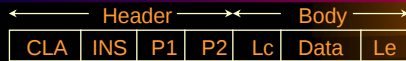
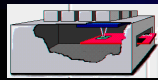
Secret Code

Mode : 0 C 0 0 : C=1() C=0()
 MPN : Maximum Presentation Number (1 ~ 7)
 SCR : Secret Code Ratification counter
 UCR : Unlock Code Reference : 0 0 0 0 L SCN

G	E	M		P	L	U	S
47	45	4D	20	50	4C	55	53
75	D0	0C	53				

SMARTCARD

□ GPK2000 Command and Response



CLA : Instruction Class (X Y)

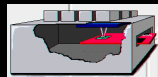
X = 0 (ISO) / 8(PCOS) Y = 0 () / 4 ()

INS : Instruction Code

P1, P2 : Parameter

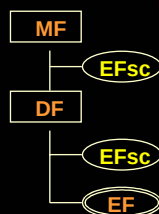
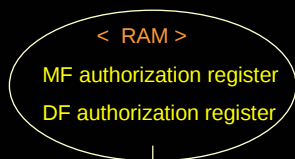
Lc : Data Length

Le : Expected Length of Data returned from Card



SMARTCARD

□ File Access Condition



- EF MF/DF
- Secret Code # (0 ~ 7)
- Secret Code(s)

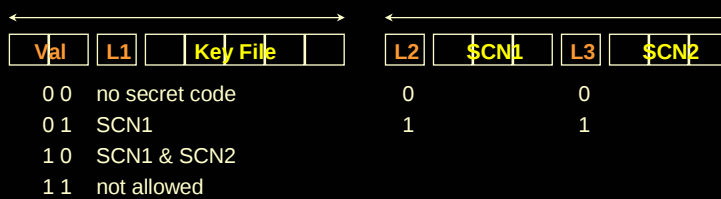
- * MF Secret Code - MF AR
- * DF Secret Code - DF AR
- * EF Access Condition Access 가

SMARTCARD

File Access Condition

	DF Level	EF Level
Group 1 AC	System file for create	Update
Group 2 AC	Common file for create	Write
Group 3 AC	None	Read

2-Byte of Access Condition in File Descriptor



SMARTCARD

File Access Method

