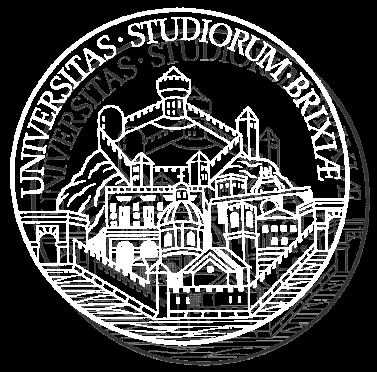
Embedding Forensics: An Ongoing Research about SIM/USIM Cards



PRISE *2007*
2° Italian Workshop on **PRI**vacy and **SE**curity
Rome, Italy, June 6, 2007

Presenter:
Ing. Antonio Savoldi
Ph.D. student
Department of Electronics for Automation
University of Brescia - Italy

Authors:
Antonio Savoldi
Paolo Gubian

Outline

- Embedding forensics definition
- SIM/USIM
  - Physical point of view
  - Logical point of view
- SIMBrush
  - Main features
  - Filesystem extraction
  - Covert channeling

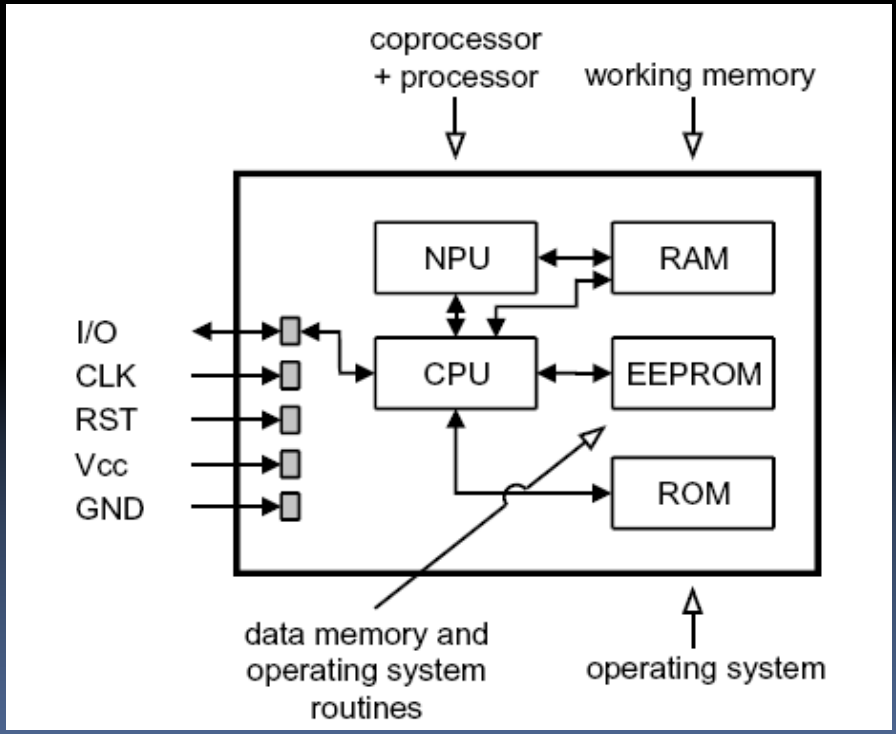
Introduction

- Embedded forensics definition:
  - It is the science of retrieving digital data from a multitude of embedded devices under forensically sound conditions
  - Cellular phones, PDAs
  - SIMs/USIMs
  - Digital cameras
  - Gaming devices
  - GPS systems
  - Unusual electronic devices
  - Small Scale Digital Devices

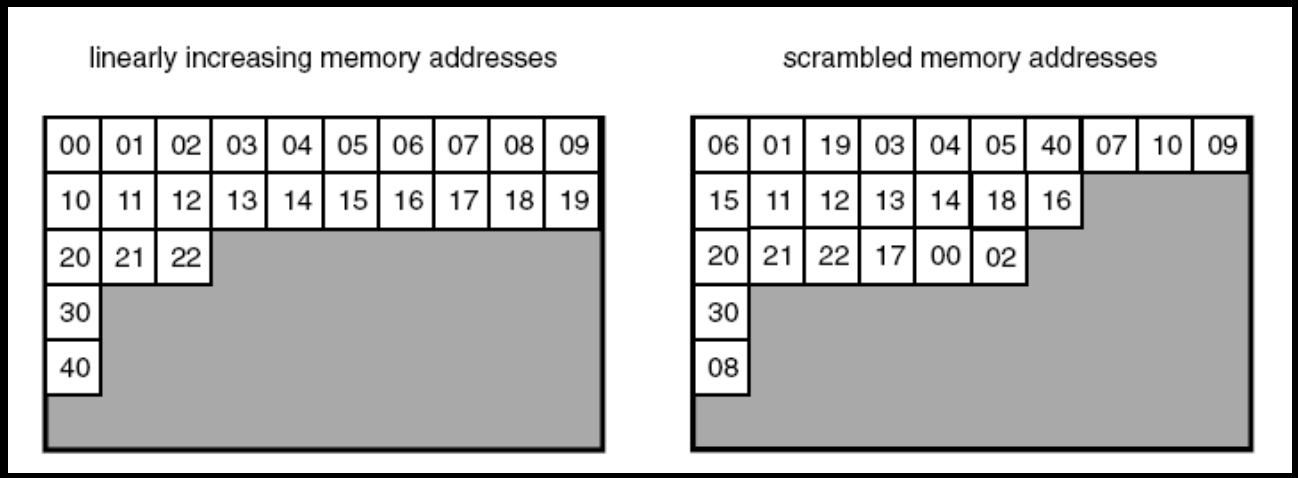
SIM/USIM: Physical Perspective

- Features about Smart Cards

- CPU
- NPU
- RAM
- EEPROM
- ROM
- I/O port

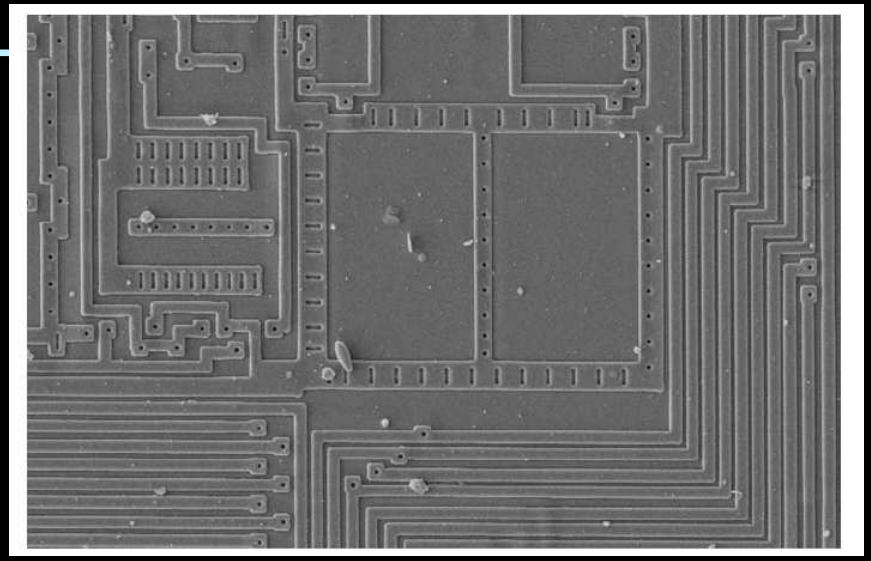


SIM/USIM: Physical Perspective



- The security of this scheme is based on secrecy of the scrambling scheme for the memory cells
- The EEPROM can also be scrambled using software
- Memory content can be encrypted using a key session

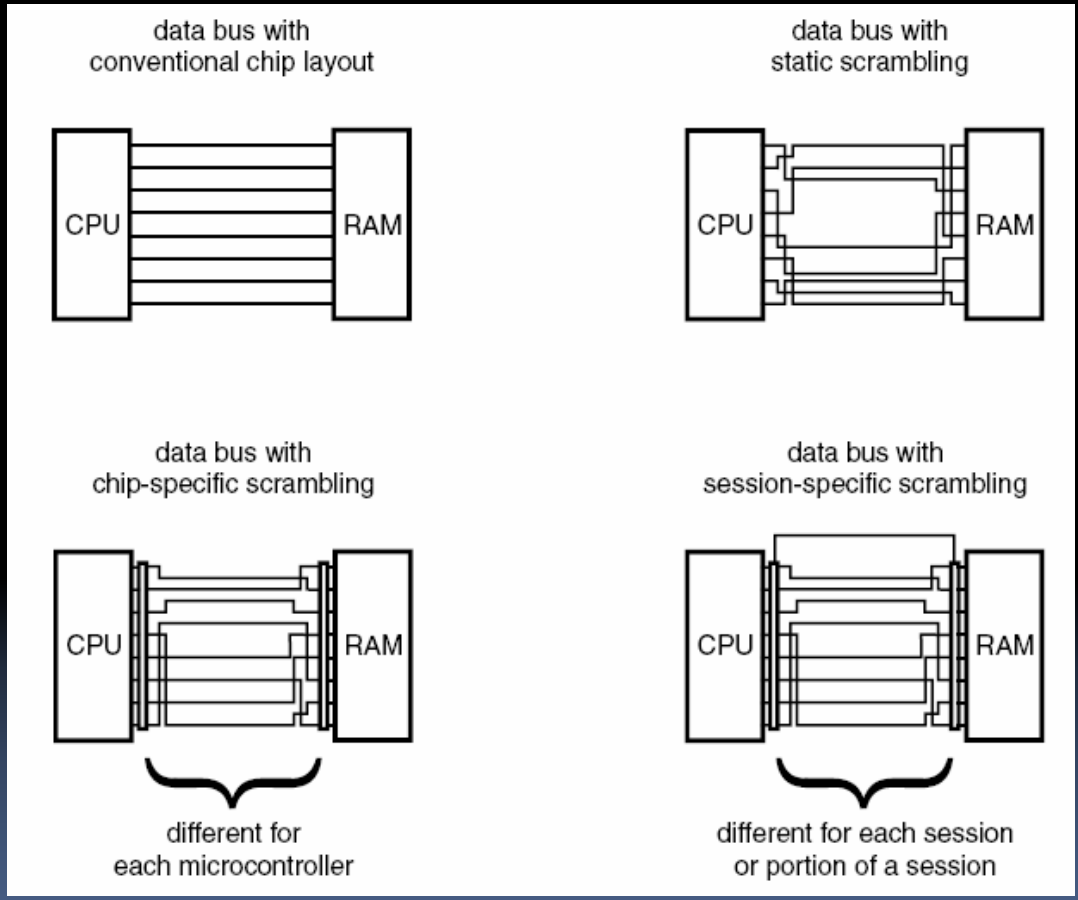
SIM/USIM: Physical Perspecti



- Protection at this stage:
  - Monitoring the passivation layer
  - Voltage monitoring
  - Frequency monitoring
  - Temperature monitoring

SIM/USIM: Physical Perspective

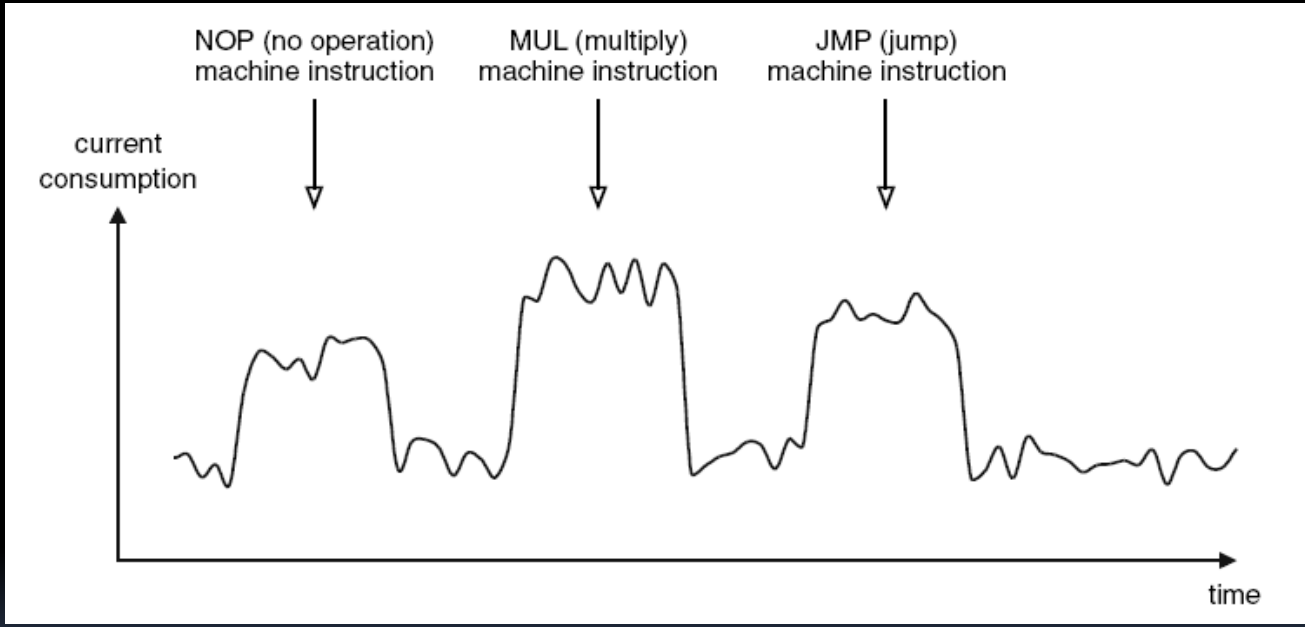
- Two types of scrambling:
  - Static
  - Dynamic
    - it is determined by using a session key



SIM/USIM: Security Issues

- It is possible to draw conclusions about the instructions being executed by a processor, by analyzing the current consumption of the processor (Kocher, Jaffe, Jun):
  - Simple Power Analysis
  - Differential Power Analysis

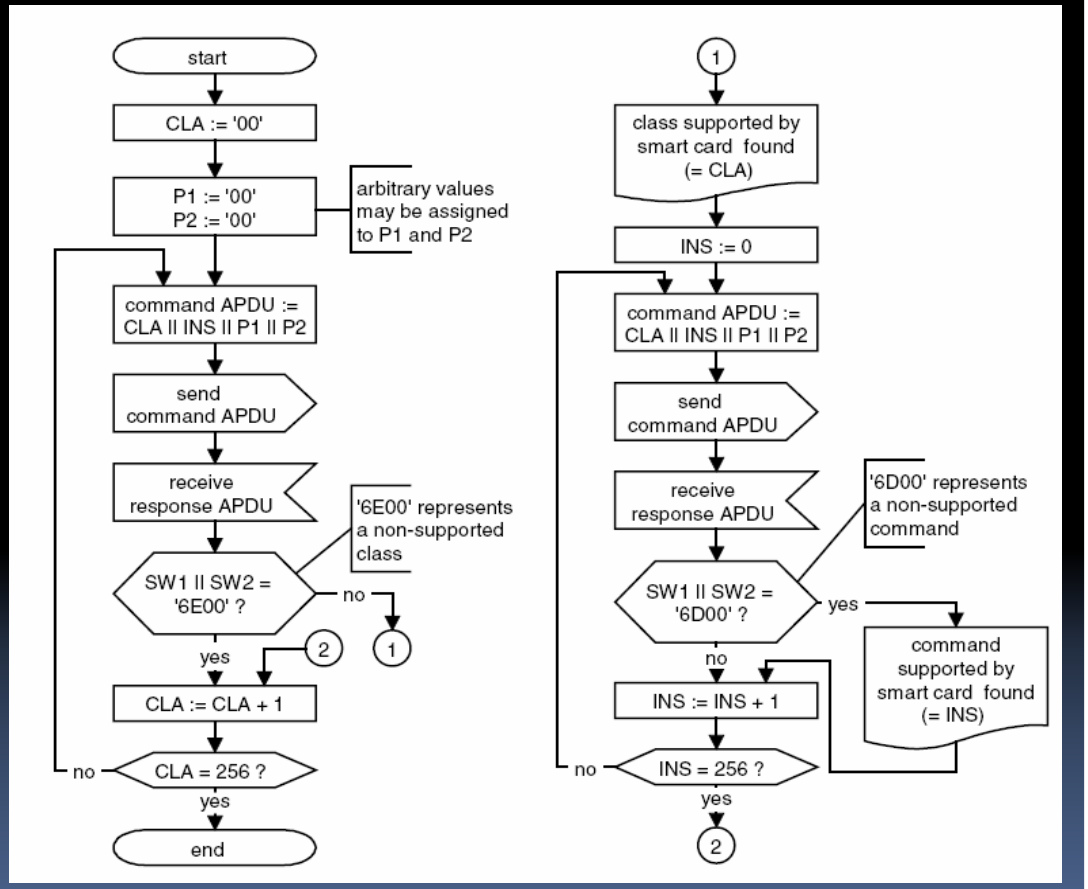
SIM/USIM: Security Issues (DPA)



- Collection of power consumption with average over series of acquisitions
  - Current consumption with known and unknown data, which are repeated many times
  - The effect of noise can be eliminated by taking the average value

SIM/USIM: Backdoors

- Basic procedure for performing an exhaustive search for all commands supported by a smart card operating system
- For each valid class (CLS) the entire addressable space is brushed

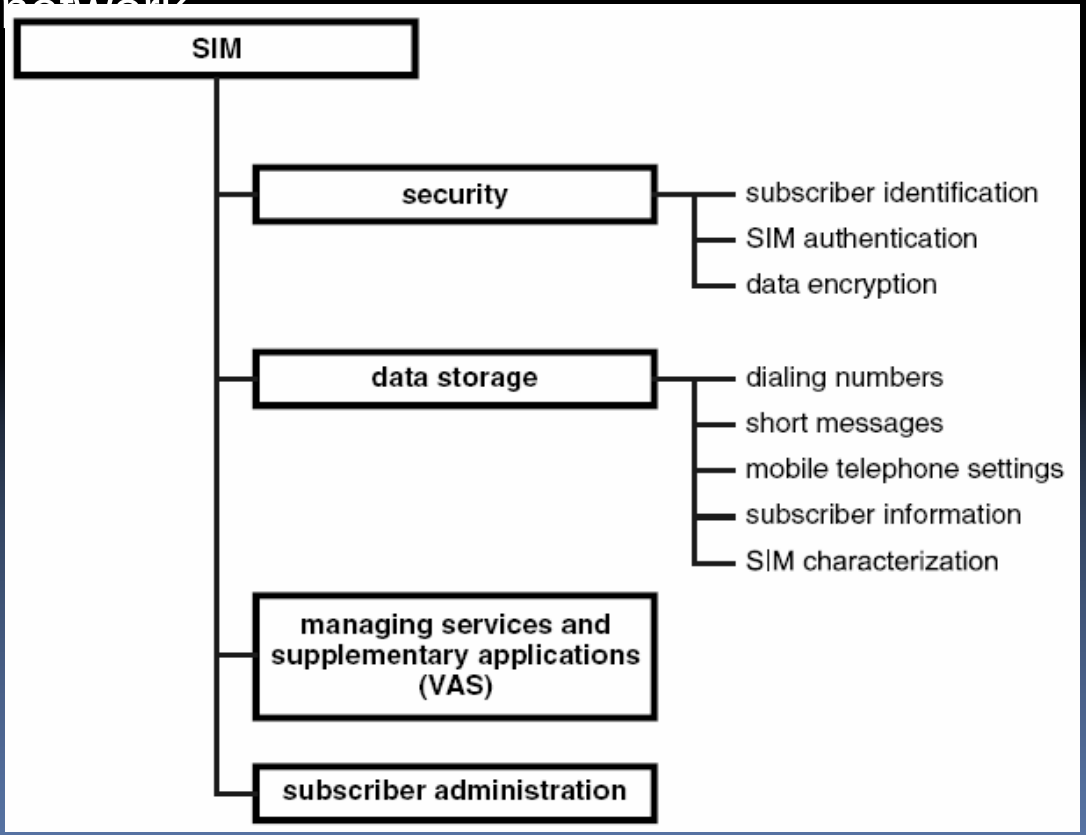


EMI Analysis

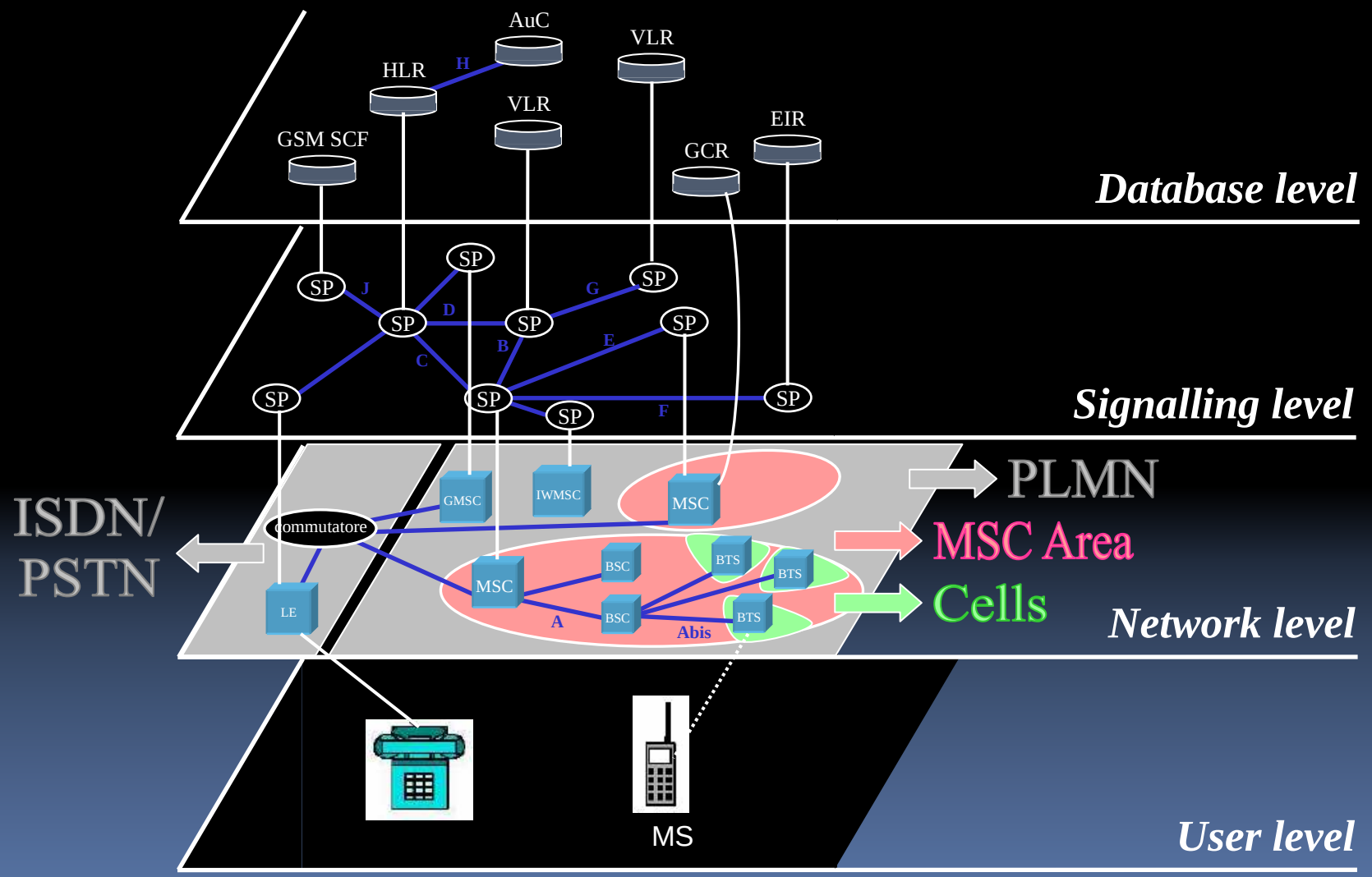
- Measuring the electromagnetic radiation of the CPU
  - Magnetic field with small strengths can be measured using SQUID (Superconducting Quantum Interference Devices)
- X-rays, ultraviolet light on EEPROM
  - It is possible to modify all S-boxes of the DES algorithm from an encryption to a linear transformation

Subscriber Identity Module

- It is an entity that contains the identity of the subscriber
  - Secure the authenticity of the mobile station with regard to the network



Infrastructural Part



Infrastructural Part

- SIMBrush is capable of extracting digital evidence from any SIM card used in GSM system
  - The most widespread system at worldwide level
- GSM system
  - Infrastructure: Database + Signalling + Network level
  - End-user: User level
    - Mobile Station = Mobile Equipment + Subscriber Identity Module
- UMTS – User Equipment = Mobile Equipment + User Service Identity Module (USIM)

Data Stored in a SIM/USIM

- **Subscriber (**IMSI, Mobile Station ISDN)
- **Acquaintances of the subscriber (**Abbreviated Dialling Numbers)
- **SMS traffic (SMS, meta content)**
- **Subscriber Location (Location Area Information)**
- **Calls (**last dialled numbers)
- **Provider (**name and accessible networks)
- **Enabled services (**services enabled for the subscriber - SST)

Filesystem

- Elementary File present in a SIM card:
  - Transparent
    - sequence of bytes
  - Linear-fixed
    - sequence of fixed length records
  - Cyclic
    - circular buffer with fixed length records
- Every file in SIM card is univocally identified by its ID (e.g. 3F00)
- Master-slave relation between SC reader and SIM card
- Standard set of commands to interact with SIM card through Interface Device (IFD)

SIM Commands

- Interaction with the OS by using APDU
- Security commands
  - Change, Disable, Enable, Unblock, Verify CHV
- Commands for operations on files
  - Read (Binary, Record)
  - Update (Binary, Record)
  - Select (File_ID)
  - Get Response

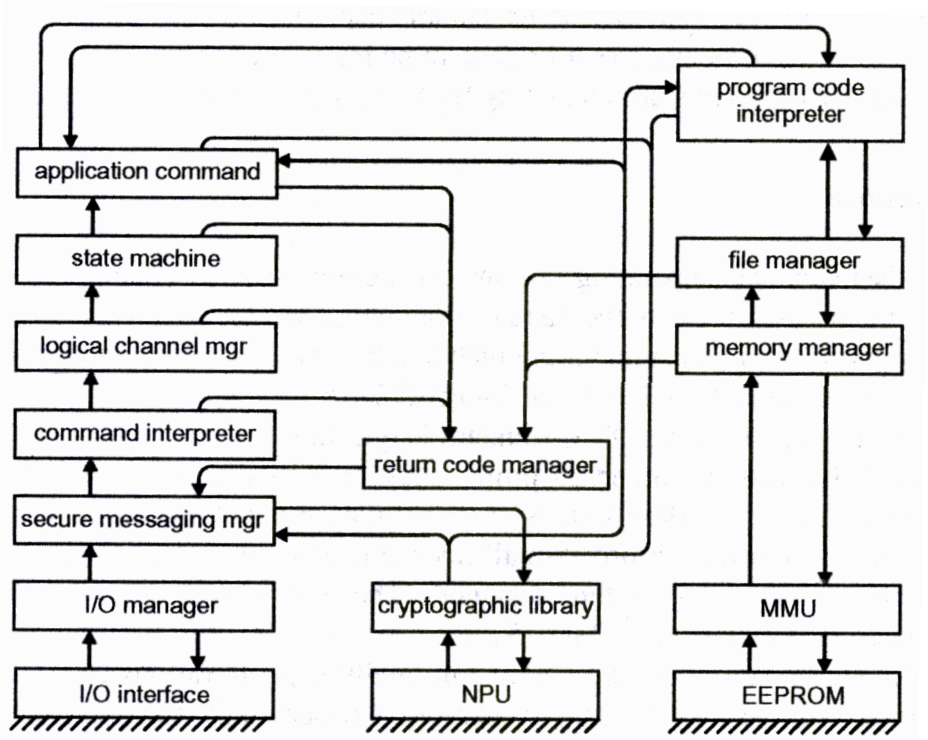
APDU (Application Protocol Data Unit)

IFD (InterFace Device)

Answer ADPU

Command ADPU

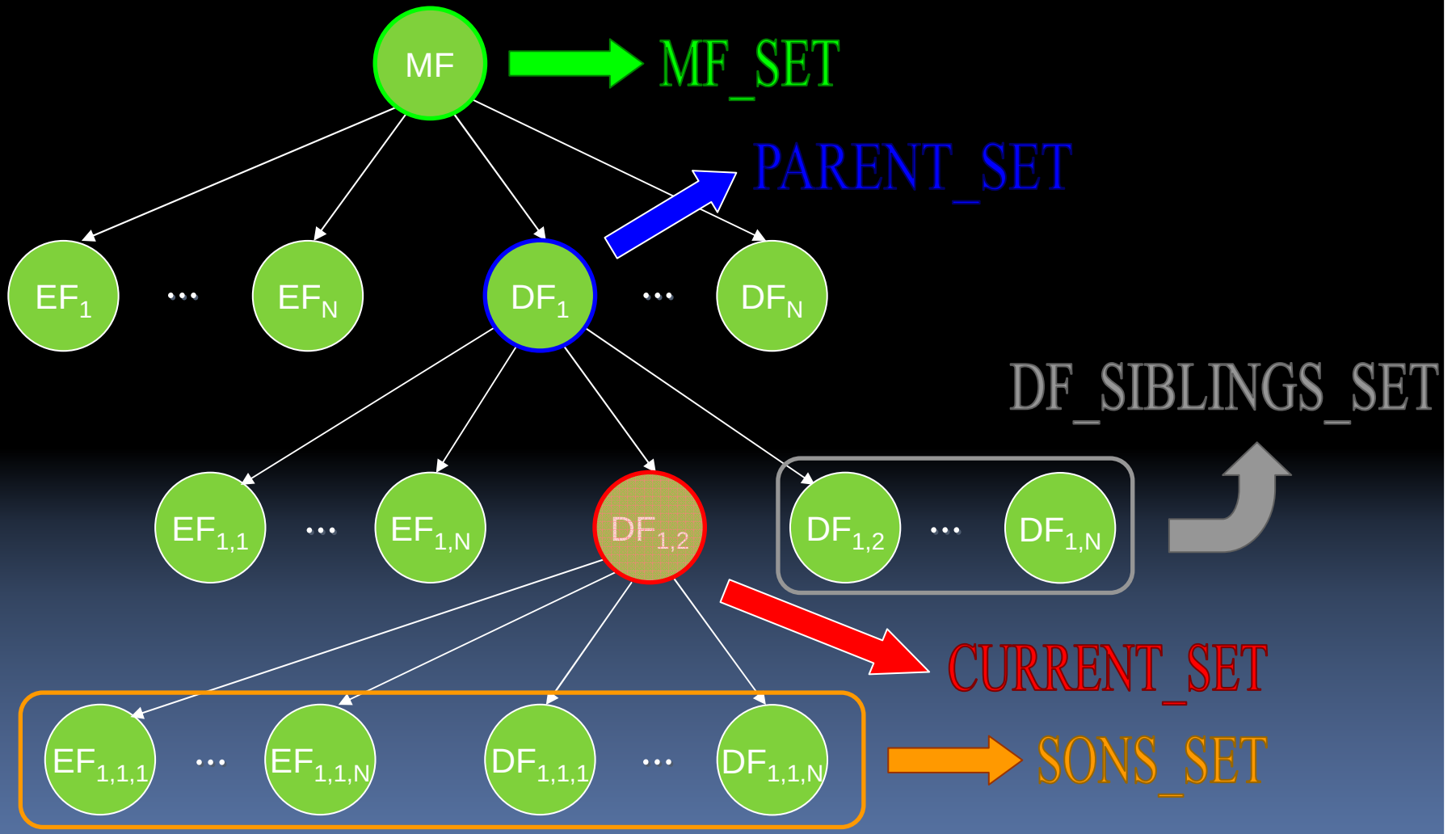
Smart-card



Schema for Filesystem Extraction

- Concept of current file and current directory
- Constraints about selectable files:
  - MF can be selected no matter what the current directory is
  - Current directory
  - Parent of current directory
  - Any DF which is an immediate child of the parent of the current directory
  - Any file which is an immediate child of the current directory

Core Algorithm (1)



Core Algorithm (2)

- Definition of file and directory set associated with preceding constraints:
  - MF_SET
  - CURRENT_SET
  - PARENT_SET
  - DF_SIB_SET
  - SONS_SET
- **SELECTABLE_SET** is created from “brushing” addressable ID space

  (0000->FFFF)
- **SELECTABLE_SET** = MF_SET U
  CURRENT_SET U
  PARENT_SET U
  DF_SIB_SET U
  SONS_SET

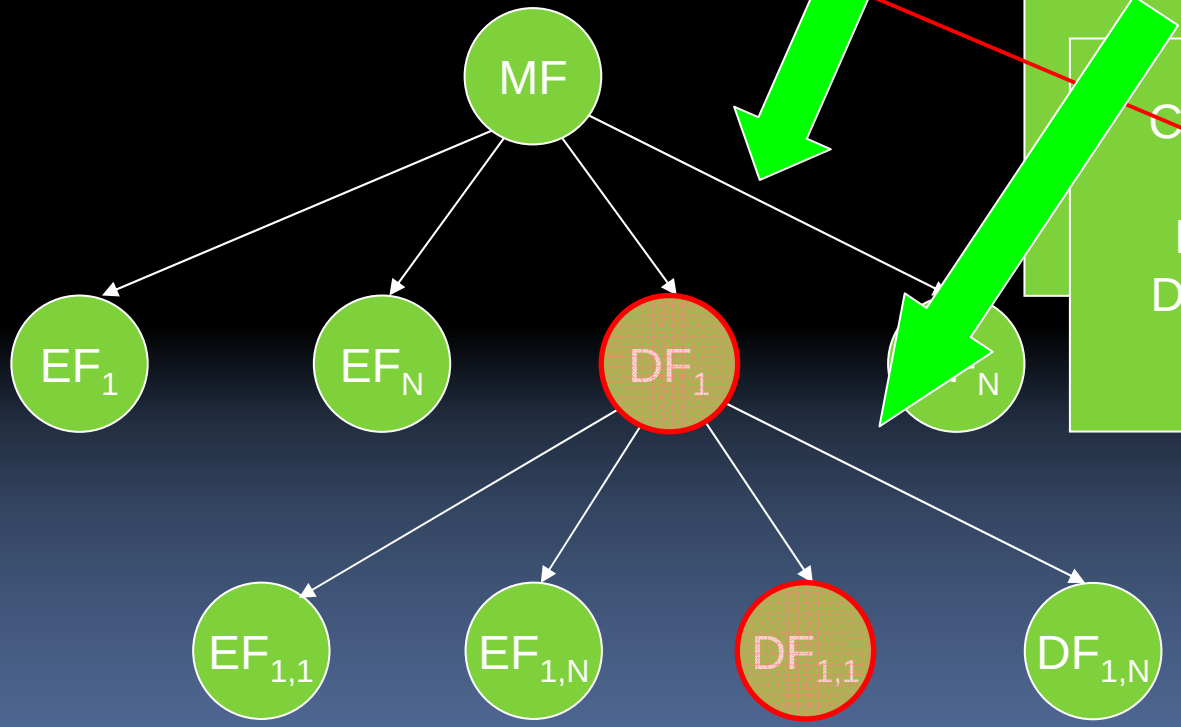
Core Algorithm (3)

- To build up the filesystem the following relation can be used because **SONS_SET** is unknown:

- SONS_SET = SELECTABLE_SET \
  (MF_SET U
  CURRENT_SET U
  PARENT_SET U
  DF_SIB_SET)

Core Algorithm (4)

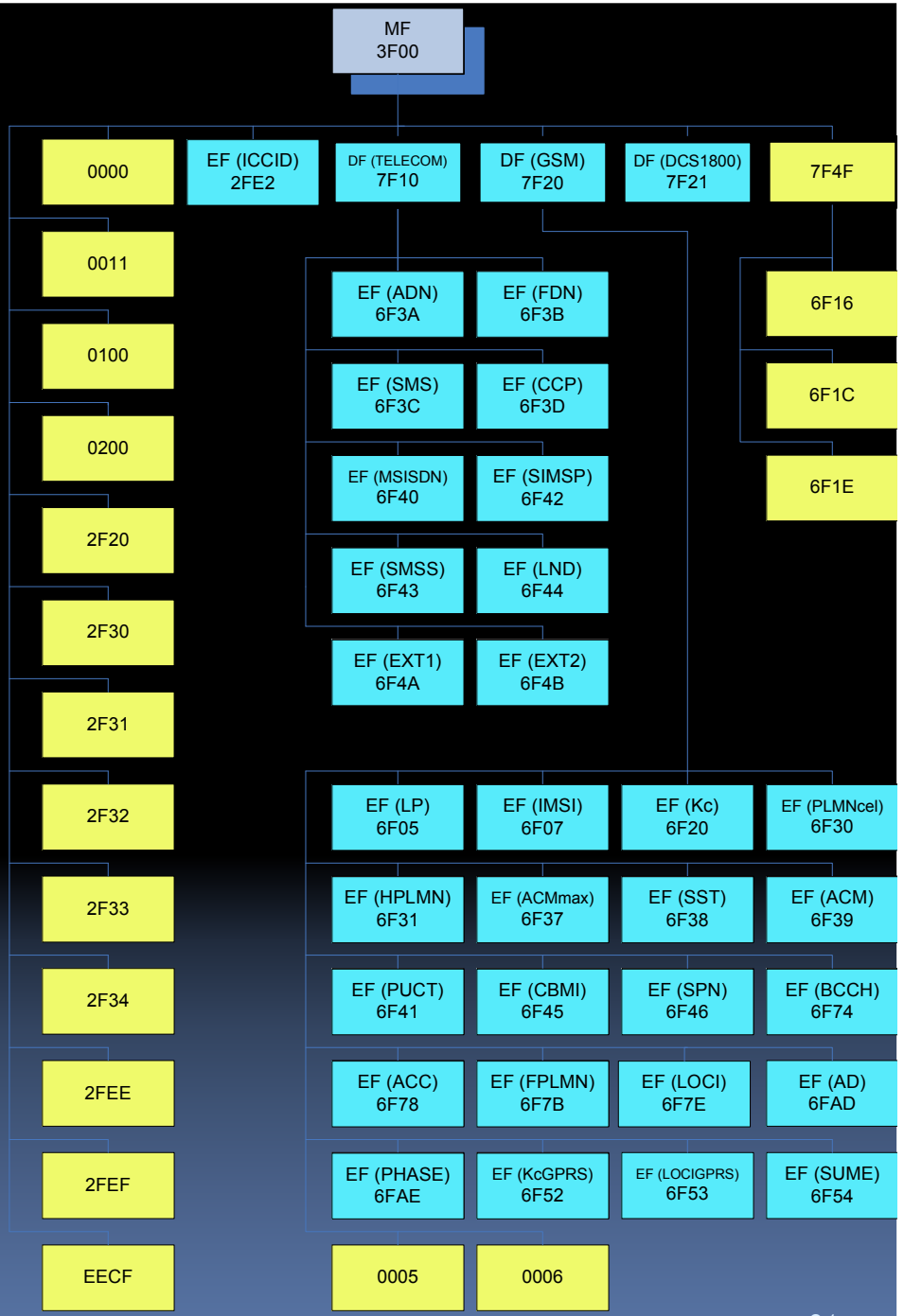
SELECTABLE_SET = {MF, DF_1, DF_2, ..., DF_N, $EF_{1,1}$, ..., $EF_{1,N}$, $DF_{1,N}$, ..., $DF_{1,N}$}



CURRENT_SET = {DF_1}
MF_SET = {MF}
PARENT_SET = {MF}
DF_BROTHERS_SET = {DF_2, ..., DF_N}

Filesystem: An Example

- Non-standard part: an issue to deal with
- By analysing the meta-content it is possible to see if some non-standard EF is rewritable with the “Update” command
- This demonstrates the possibility to use the SIM/USIM card as a covert channel



Results

- SIMbrush has been tested against several SIM cards:
  - 8KB EEPROM GSM SIMs
  - 128KB GSM/GPRS SIMs
  - USIMs
- Extraction time: T = K*N
  - K is empirically determined to be 20 minutes
  - N is the number of DF (for each DF the whole addressable space is brushed)
- Output is printed in XML format
  - Simple template that replies extracted filesystem
- Digital integrity assured with hash of sensible content extracted from SIM-card (sha1)

File Allocation Table (EAT)

ID	Name	File Type	Privileges	Structure	Father	Size [byte]
3F00	**MF**	**MF**	—	—	—	—
2F00	NS	EF	ALW[2],ALW,ADM,NEV,NEV,NEV	linear fixed	3F00	46
2F05	ELP	EF	ALW,CHV1,NEV,NEV,NEV	transparent	3F00	4
2F06	NS	E			3F00	330
2FE2	ICCID	E			3F00	10
2FE4	NS	E			3F00	35
2FE5	NS	E			3F00	6
2FFE	NS	E			3F00	8
7F10	**DFTELECOM**	**D**			**3F00**	—
5F3A	**NS**	**D**			**7F10**	—
4F21	NS	E			5F3A	500
4F22	NS	E			5F3A	4
5FFF	**NS**	**D**			**7F10**	—
1F00	NS	EF	ADM,ADM,NE ,ADM	transparent	5FFF	105
1F01	NS	EF	ADM,ADM,NE ,ADM	transparent	5FFF	175
1F02	NS	EF	CHV1,CHV1,N /,NEV	transparent	5FFF	11
1F03	NS	EF	ALW,ADM,NE NEV	linear fixed	5FFF	40
1F04	NS	EF	ALW,CHV1,NE ,NEV	transparent	5FFF	4
1F05	NS	EF	ADM,ADM,NE ,ADM	linear fixed	5FFF	640
1F06	NS	EF	ADM,ADM,NE ,ADM	linear fixed	5FFF	420
1F07	NS	EF	CHV1,ADM,NE I,ADM	transparent	5FFF	20
1F08	NS	EF	CHV1,CHV1,N /,NEV	transparent	5FFF	175
1F09	NS	EF	CHV1,CHV1, ADM	transparent	5FFF	100
1F0A	NS	EF	ADM,ADM,NE ,ADM	linear fixed	5FFF	16
1F0B	NS	EF	ADM,ADM,NEV DM,ADM	transparent	5FFF	16
1F0C	NS	EF	CHV1,CHV1,NEV,CHV1,CHV1	linear fixed	5FFF	34
1F1E	NS	EF	CHV1,CHV1,NEV,ADM,ADM	linear fixed	5FFF	70
1F1F	NS	EF	CHV1,CHV1,NEV,ADM,ADM	linear fixed	5FFF	70
1F20	NS	EF	CHV1,ADM,NEV,ADM,ADM	linear fixed	5FFF	128
1F21	NS	EF	CHV1,CHV1,NEV,ADM,ADM	linear fixed	5FFF	1280
1F22	NS	EF	CHV1,CHV1,NEV,ADM,ADM	linear fixed	5FFF	340
1F23	NS	EF	CHV1,CHV1,NEV,ADM,ADM	linear fixed	5FFF	500

Hidden Part in which it is possible to hide arbitrary data

Non-standard Part

- **WNSP**: Writable Non-standard Part
- **NSP**: Non-standard Part of the filesystem
- **TES**: Total Engaged Space

Table 6. WNSP regarding some of the analyzed SIM/USIM.

#	Provider	Country	EEPROM	Phase	Services	WNSP	NSP	TES
1	TIM	Italy	16KB	2	GSM	0	151	6997
2	Vodafone	Italy	32KB	2	GSM	0	531	8743
3	BLU	Italy	64KB	2+	GSM	0	21122	31087
4	Omnitel	Italy	64KB	2+	GSM	0	17427	25689
5	Wind	Italy	64KB	2+	GPRS	96	4737	22651
6	TIM	Italy	128KB	2+	GPRS	16549	42859	56887
7	TIM	Italy	128KB	2+	GPRS	12478	25112	45729
8	H3G	Italy	128KB	3	UMTS	107	21290	30826

Discovering the Non-standard part

- Some guidelines:
  - Extract all the observable memory of SIM/USIM
  - Creation of the FAT
  - Analysis of the Writable Nonstandard part of the filesystem
  - Descrambling the hidden message
    - Application of the classical techniques belonging to steganalysis field

Lesson Learnt

- Every non-standard EF with CHV1/CHV2 access privileges on the Update command is writable
  - Concrete possibility to hide plenty of information
  - The SIM/USIM can become a real Covert Channel
- A standard 128 Kbytes SIM card can have approximately 17 Kbytes of hidden writable space
  - This part of the filesystem is not findable by using current forensics tools
  - WNSP (Writable Non-standard Part)