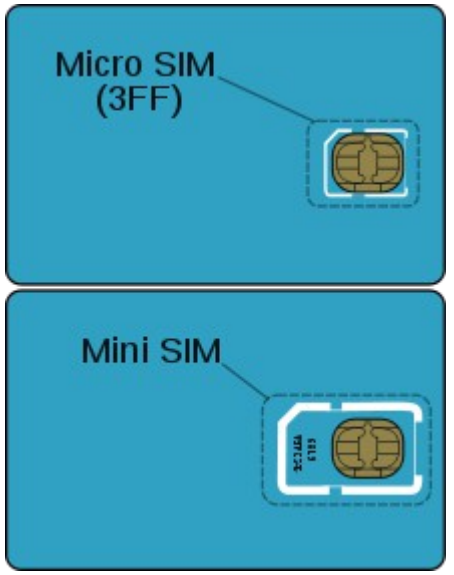


Mobile telephones

SIM (Subscriber Identity Module)

UICC (Universal Integrated Circuit Card)

SIM 1

- A smart card used for identifying the cell phone
- Protected by
  - A PIN (Personal Identification Number)
  - A PUK (Personal Unblocking Code)
- Also includes other parameters of the user such as it's IMSI and MSISDN (full telephone number)
  - Allows the cell phone to be identified and operate on the network
- Essential component to GSM and WCDMA cell phones
  - CDMA have a CSIM card (same form factor)
- Contain information particular to the user which uniquely identifies the subscriber
- The SIM is a UICC (Universal Integrated Circuit Card)

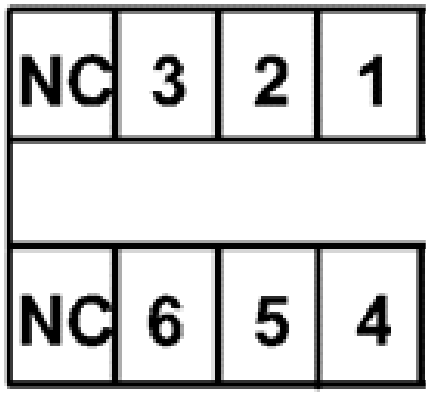
SIM 2

http://www.forensicswiki.org/wiki/SIM_Cards
http://en.wikipedia.org/wiki/Smart_card

- An UICC SIM smart card contain
  - CPU
  - RAM
  - ROM for OS
  - EEPROM for storage, 32/64 kB are common
  - I/O circuits
  - http://en.wikipedia.org/wiki/UICC

- Stores
  - ICCID (card identity/serial nr.)
  - IMSI (International Mobile Subscriber Identity)
  - User data as last dialed numbers, SMS, phone book etc.
  - Operator data - network configuration information
  - And alot more!
- Defined by international standards - ETSI
  - European Telecommunications Standards Institute

SIM physical interface



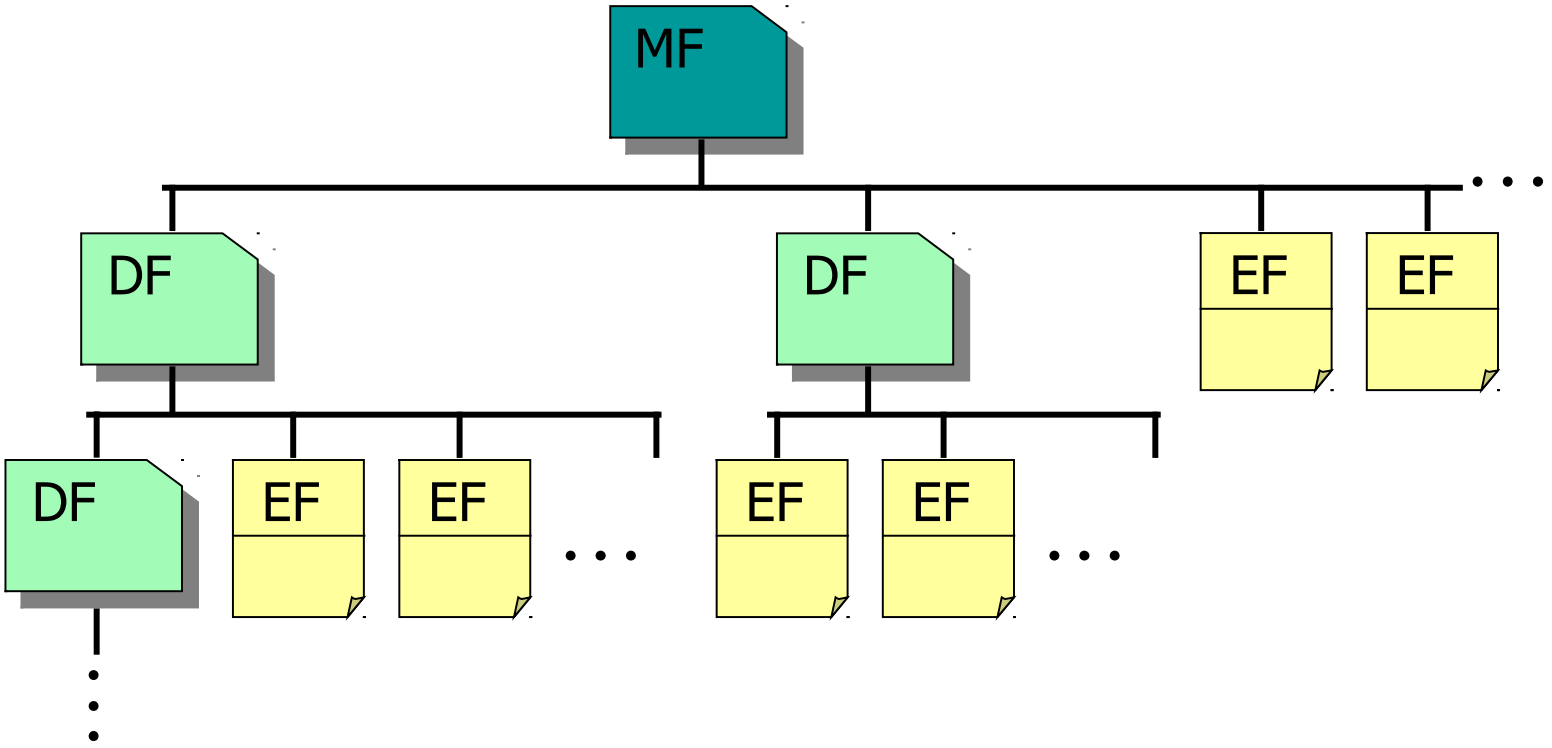
1- Vcc (5V)
2- Reset
3- Clock
4- GND
5- Vpp Programing voltage
6- Data I/O

Usually ICCID and subscriber number is printed on back

SIM file system

- Hierarchically organized file system
  - Stores names and phone numbers, received and sent text messages etc.
  - Security information
  - Network configuration information
- Three types of files
  - Master Files (**MF**)
  - Dedicated Files (**DF**)
  - Elementary Files (**EF**)
- Allows for quick porting/change from one phone to another

Smart Card File System (ISO 7816-4)

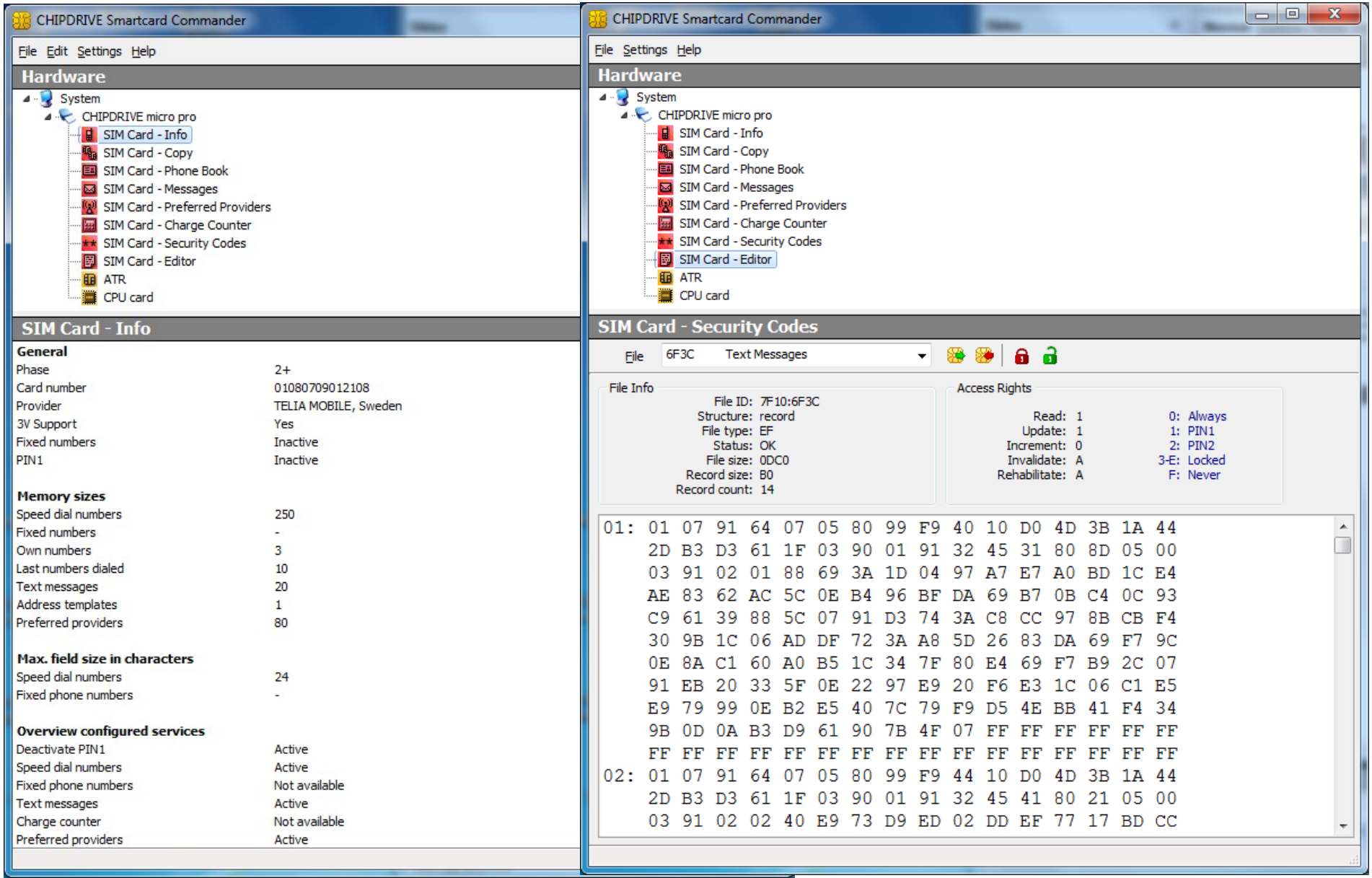


MF Master File (root directory, must always be present)

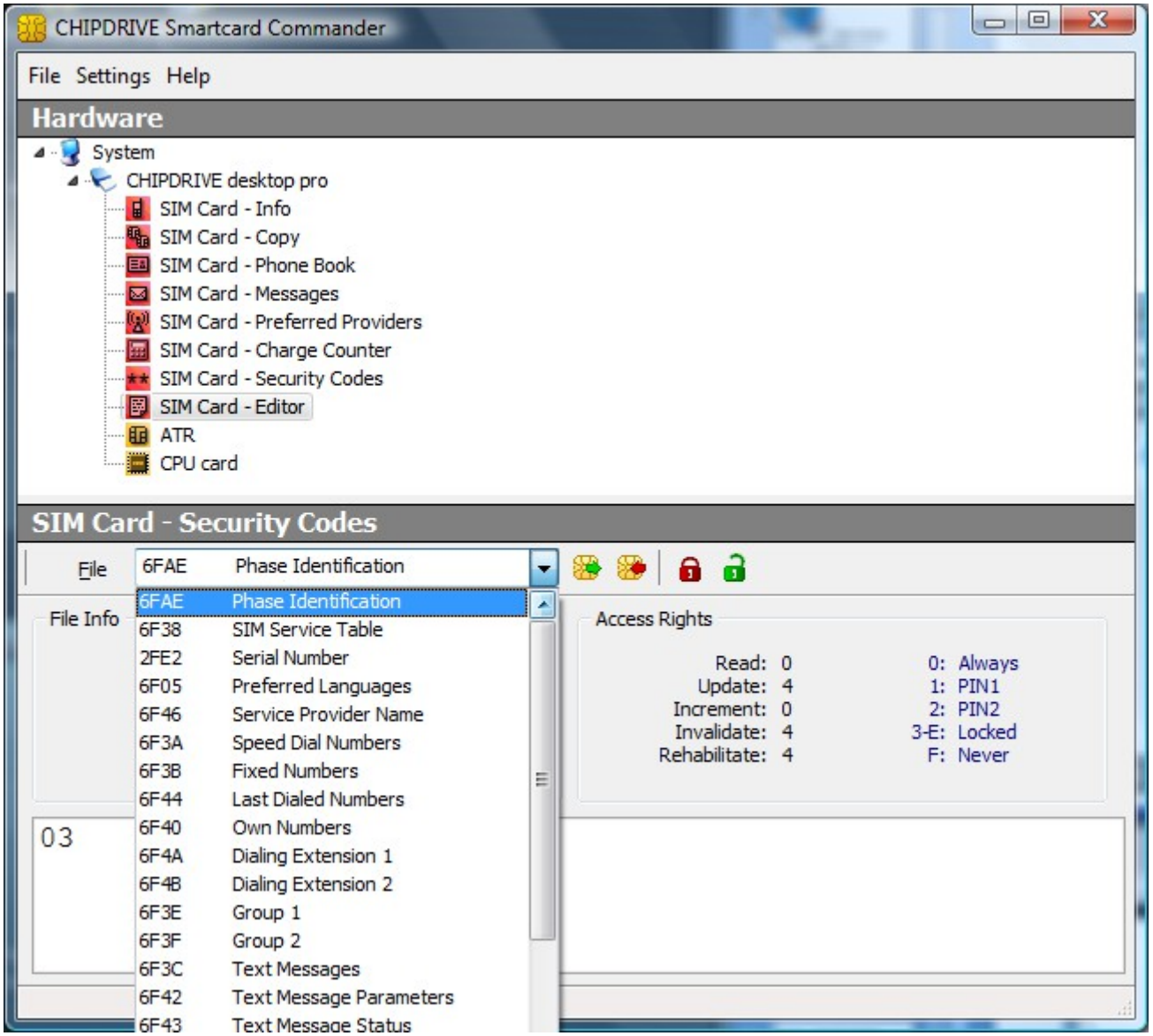
DF Dedicated File (directory file, can contain directory and data files)

EF Elementary File (data file)

Chipdrive Smartcard Commander

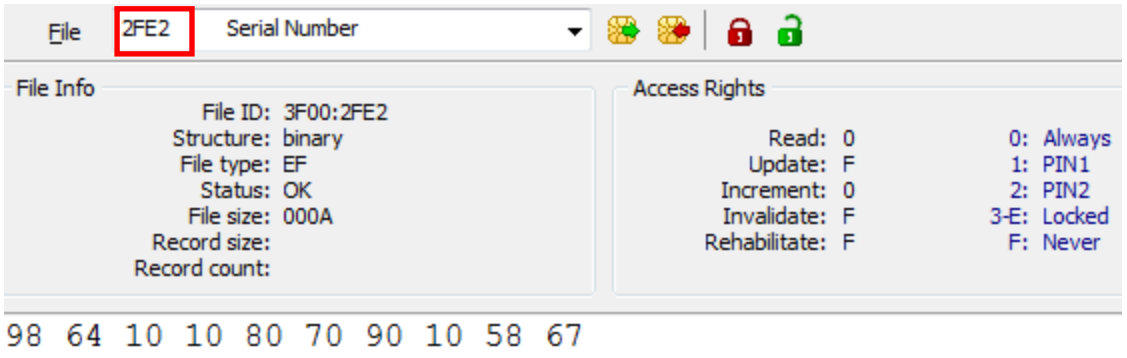


Chipdrive Smartcard Commander



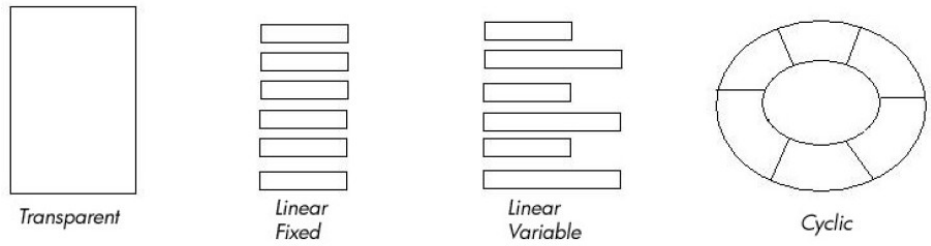
SIM structure

- File ID is used to address/identify each specific file
  - 3F** = Master File
  - 7F** = Dedicated File
  - 2F** = Elementary File under Master File (only one EF - ICCID)
  - 6F** = Elementary File under Dedicated File
- File ID rules
  - File ID shall be assigned at the time of creation of the file
  - Two files under the same parent shall NOT have the same file ID
  - A child and any parent, anywhere in the hierarchy, shall NOT have the same file ID



Logical Model of the SIM

- Master Files (MF)
  - Unique mandatory file containing access conditions and optionally dedicated and elementary files
  - Analogous to root directory
- Dedicated Files (DF)
  - A functional grouping of files consisting of itself and all those files which contain this DF in their parental hierarchy
  - A DF consists only of a header
- Elementary Files (EF)
  - Composed of a header and body part which contain the data
  - 3 structures used by GSM
    - Transparent
    - Linear Fixed
    - Cyclic



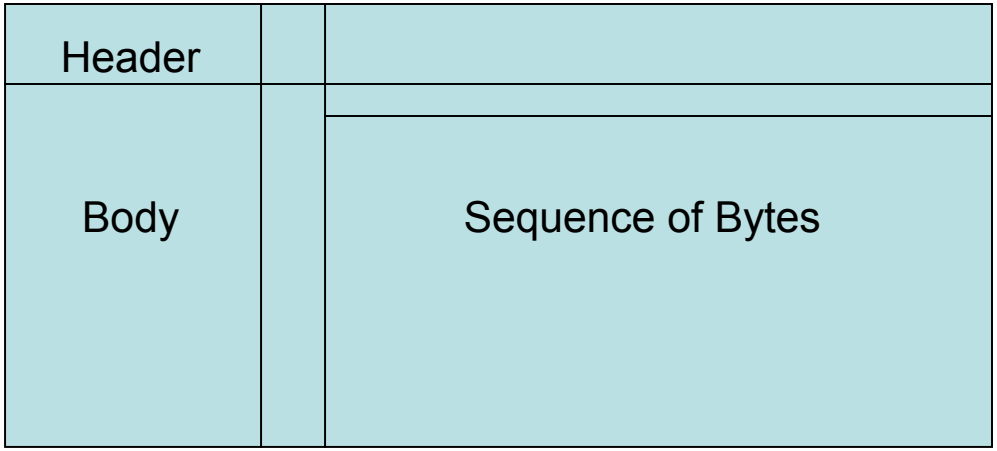
Elementary File Variations

Transparent EF

- Consists of a sequence of bytes
- When reading or updating, the sequence of bytes to be acted upon is referenced by a relative address (offset), which indicates the start position (in bytes), and the number of bytes to be read or updated
- The first byte of a transparent EF has the relative address ’00 00’
- The total data length of the body of the EF is indicated in the header of the EF
- This structure can also be referred to as **“binary”** in GSM

Transparent EF structure

- Examples include:
  - ICCID
  - Language Preference
  - IMSI
  - LOCI
  - Ciphering Key Kc
  - PLMN
  - HPLMN
  - ACM
  - SIM Service Table



Linear Fixed EF

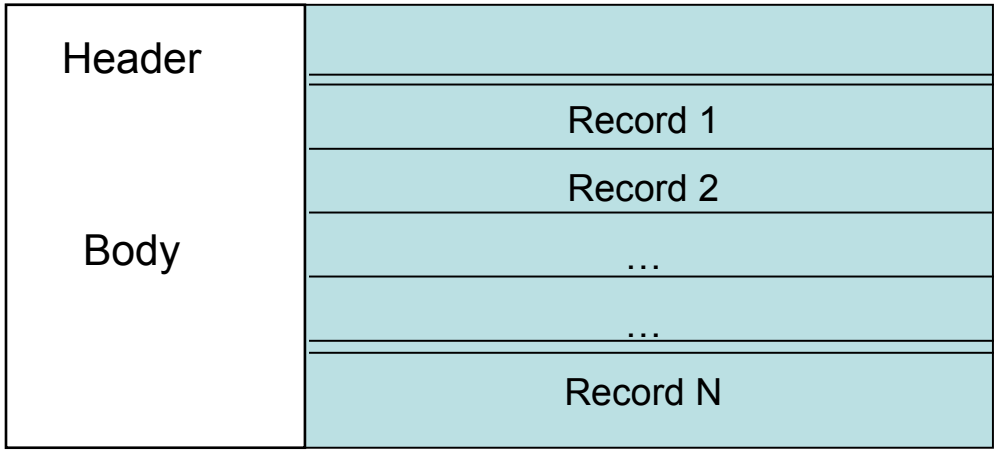
- An EF with linear fixed structure consists of a sequence of records all having the same (fixed) length
- The first record is record number 1
- The length of a record as well as this value multiplied by the number of records are indicated in the header of the EF
- It is not possible, at present, to have more than **255 records** in a file of this type, and each record cannot be greater than **255 bytes**
- This structure can also be referred to as **"record"** in GSM

Linear Fixed EF

- There are several methods to access records within an LF EF
  - Absolutely using the record number
  - When the record pointer is not set it shall be possible to perform an action on the first or last record
  - When the record pointer is set it shall be possible to perform an action on this record, the next record (unless point at last), or the previous record (unless point at first)
  - By identifying a record using pattern seek starting:
    - Forward from BOF
    - Forward from Pointer
    - Backward from EOF
    - Backward from Pointer

Linear Fixed EF structure

- Examples include:
  - Speed Dial Numbers
  - Fixed Dialing Numbers
  - MSISDN or Own Numbers
    - The full telephone number of the SIM card
    - Country Code + National dest. Code + Subscriber number
  - Capability Configuration Parameters
  - Short Messages
  - Short Message Service Parameters

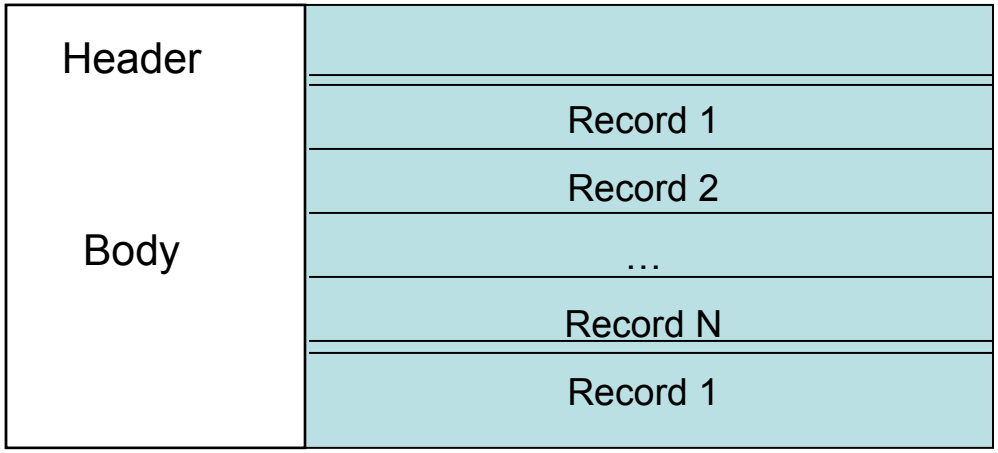


Cyclic EF

- Used for storing records in chronological order
- When all records exhausted, next storage of data overwrites oldest information
- Consists of a fixed number of records with the same (fixed) length
- Last record is linked to first record
- 255 records is the maximum number
- 255 bytes is the maximum size of a record

Cyclic EF structure

- Examples include:
  - Accumulated Call Meter
  - Last Dialed Numbers
  - Charge Counter



Some EFs Header Codes

All may not be implemented on SIM
Names may be different

2F E2 = ICC Identification (Int. Circuit Card)
6F 05 = Language Preference
6F 07 = IMSI (Int. Mobile Subscriber ID)
6F 20 = Session ciphering Key Kc (64bit)
6F 30 = PLMN selector (Public Land Mobile Net)
6F 31 = HPLMN search period (Home PLMN)
6F 37 = ACM max. value (Accumulate Call Meter)
6F 38 = SIM service table (Subscriber Id Module)
6F 39 = ACM (Accumulated Call Meter)
6F 3E = Group identifier level 1
6F 3F = Group identifier level 2
6F 41 = PUCT (price per unit charge)
6F 45 = CBMI (cell broadcast msg id)
6F 46 = Service provider name
6F 74 = BCCH (Broadcast Control Channels)
6F 78 = ACC (Access Control Class)
6F 7B = Forbidden PLMNs
6F 7E = LOCI (Location Info)

Some EFs Header Codes

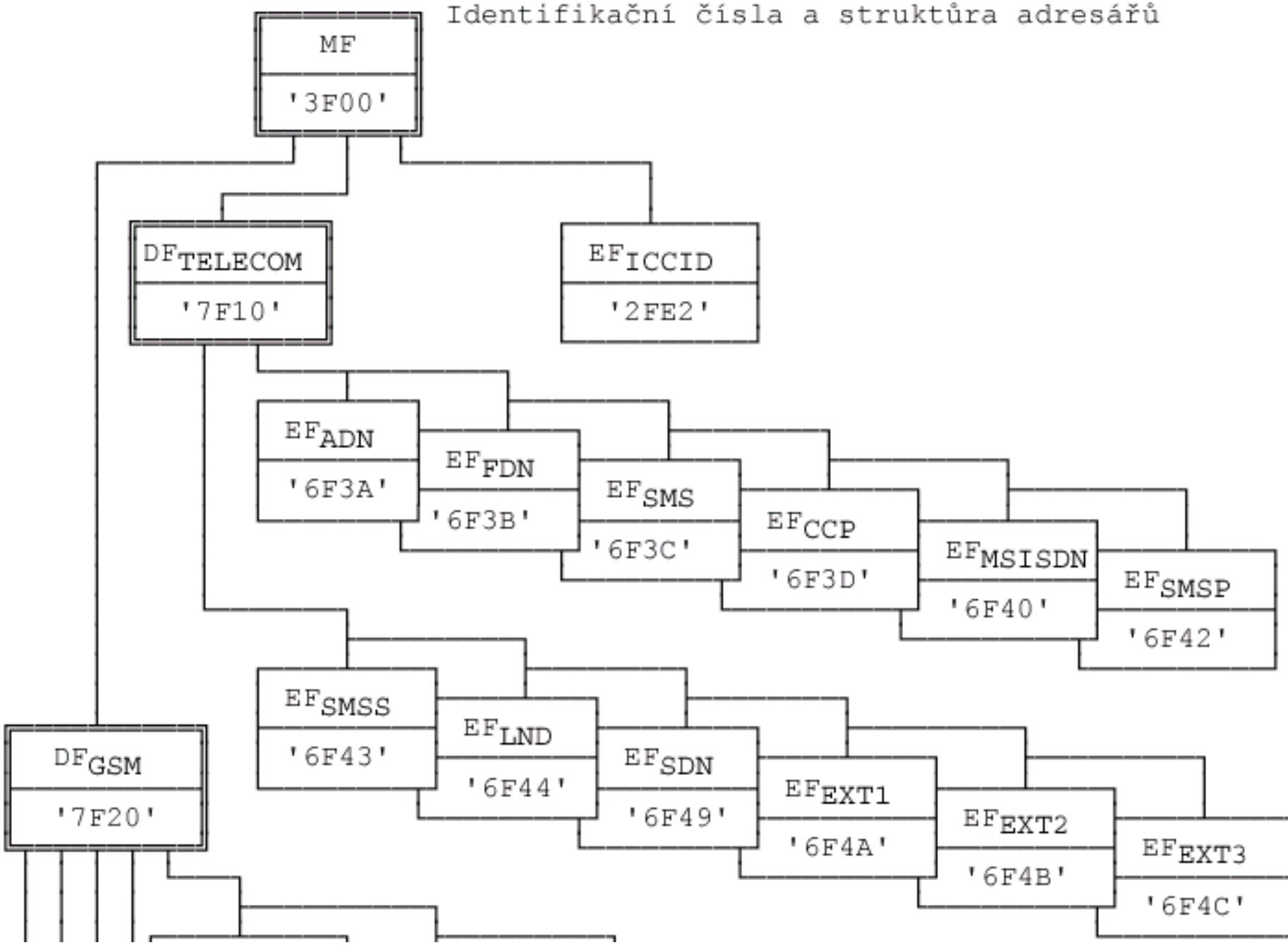
All may not be implemented on SIM
Names may be different

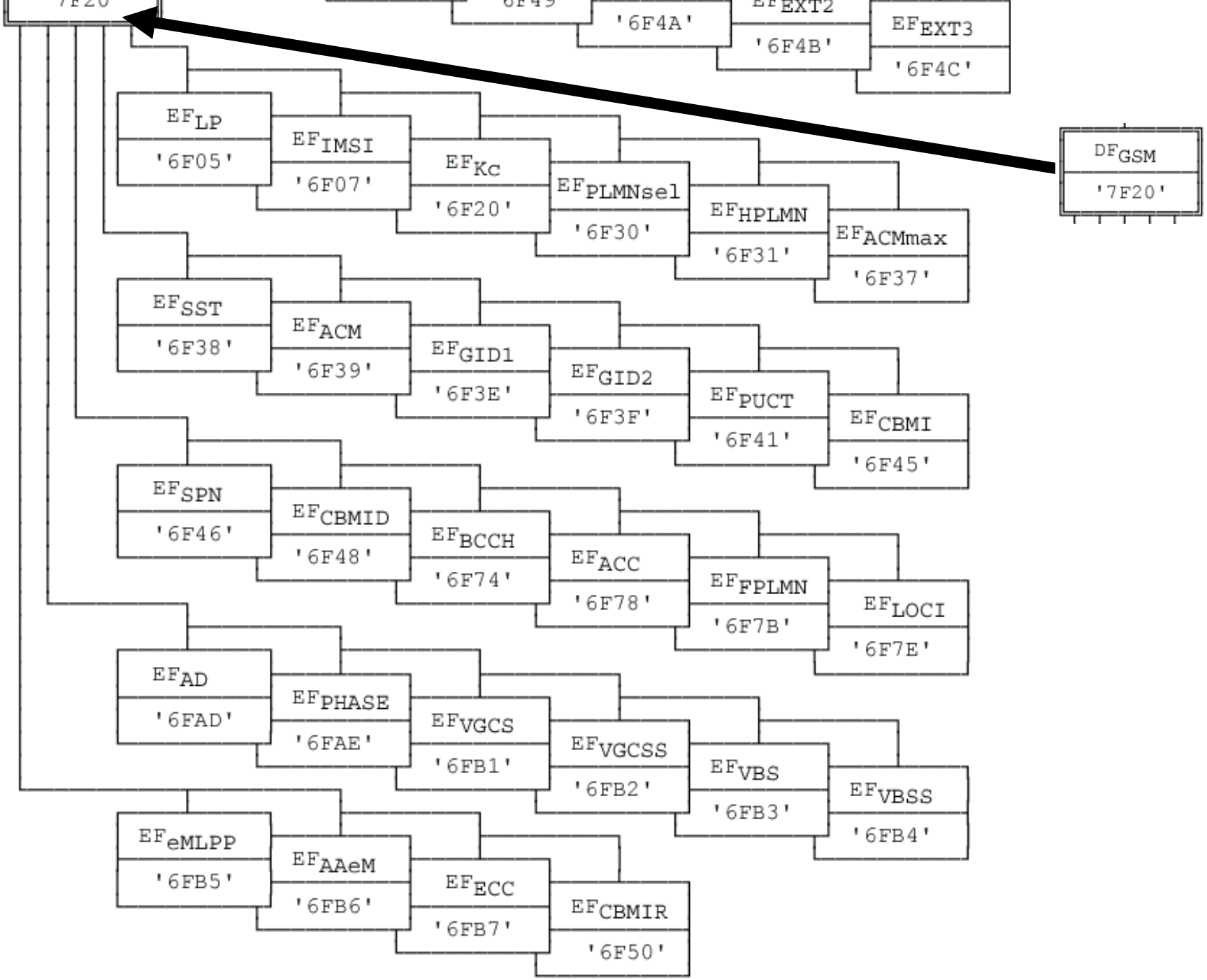
6F AD = Administrative data
6F AE = Phase identification
6F 3A = Abbreviated dialing numbers
6F 3B = Fixed dialing numbers
6F 3C = Short messages

6F 40 = MSISDN storage
6F 42 = SMS params
6F 43 = SMS status
6F 44 = Last dialed numbers
6F 4A = Extension 1
6F 4B = Extension 2

- DFTelecom – Efs common features
- DFGSM – Efs that are exclusive for GSM

Identifikační čísla a struktůra adresářů




EF EXT2 '6F4A'
EF EXT3 '6F4B'
'6F4C'
DF GSM '7F20'
EF LP '6F05'
EF IMSI '6F07'
EF Kc '6F20'
EF PLMNsel '6F30'
EF HPLMN '6F31'
EF ACMmax '6F37'
EF SST '6F38'
EF ACM '6F39'
EF GID1 '6F3E'
EF GID2 '6F3F'
EF PUCT '6F41'
EF CBMI '6F45'
EF SPN '6F46'
EF CBMID '6F48'
EF BCCH '6F74'
EF ACC '6F78'
EF FPLMN '6F7B'
EF LOCI '6F7E'
EF AD '6FAD'
EF PHASE '6FAE'
EF VGCS '6FB1'
EF VGCSS '6FB2'
EF VBS '6FB3'
EF VBSS '6FB4'
EF eMLPP '6FB5'
EF AAeM '6FB6'
EF ECC '6FB7'
EF CBMIR '6F50'

Location Information File - 6F7E

- **LOCI** contains:
  - TMSI (Temporary Mobile Station Identity)
  - TMSI Time
  - LAI (Location Area Identity)
    - (CC) Country Code – 2 digits, Mobile Network Code (MNC) – up to 3 digits, Location Area Code (LAC) up to 5 decimal digits
    - 46-01-6013 or with names and in hex: Sweden:Telia:0x177d
  - Location Update Status
- Network Operator specific
- Data retained when phone powered down
- Updated as phone moves from one location to another
- Location of phone when last used
- Location Areas can contain many cells
  - LOCI DOES NOT DETAIL WHICH CELL!
- Cell-ID data is not stored on SIM

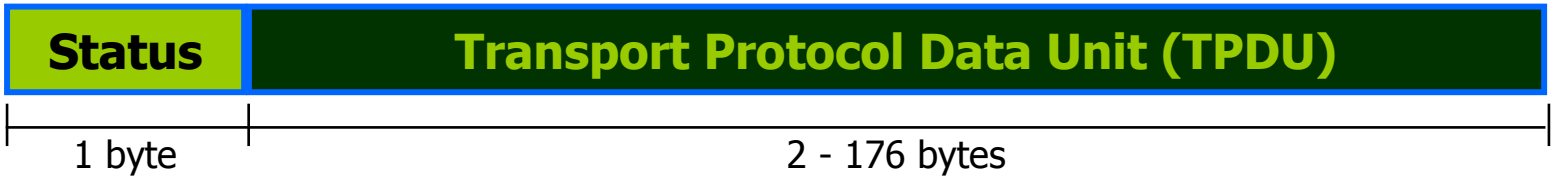
SIM numbers

- Serial Number – 2FE2
  - ICCID (Integrated Circuit Card Identifier)
  - Corresponds to the number printed on the surface of the SIM
  - Identifies the SIM
    - Only EF at MF Level
- IMSI – 6F07
  - International Mobile Subscriber Identity
  - Unique ID for every subscription on the network
  - IMSI = MCC + MNC + MSIN
- MSISDN – 6F40
  - Mobile Station International Subscriber Directory Number
    - Users unique phone number (MSISDN = CC + NDC + SN)
    - Usually the last 3 digits in ICCID and SN are the same
  - May have more than one…

SIM SMS - 6F3C

File	Purpouse	Size
SMS	The text messages	n * 176 bytes
SMSP	Text message parameters	variable
SMSS	Text message status	variable

- Short Message Service – Store received/sent messages
- Most SIM's have 10-20 slots for storing messages
  - Usually the storage of SMS is on the mobile device



SIM SMS status byte values

Value	Interpretation
0x00	Unused
0x01	Mobile terminated message, read
0x03	Mobile terminated message, unread
0x05	Mobile originated message, sent
0x07	Mobile originated message, not sent

- If user deletes a message, only status flag is changed – to unused 0x00
  - If the message has not been overwritten, the message in a slot can be recovered and translated

SIM SMS TPDU

- The TPDU consists of the following elements
  - ISDN Number of the SMS service center
  - ISDN Number of the sender (or recipient, depending on status) of the message
  - Date and time (in seconds) message received by SMS service center (time of the clock at the SMS service center)
  - Phonebook number on phone (ie. Inbox, Outbox)
  - The message itself
    - Encoding varies between manufacturers
    - Most common is 7-bit packed as defined by the GSM standard
    - Message is optimised for streaming onto the SIM
    - Unused bytes contain FF hex value

http://www.dreamfabric.com/sms/

Last Dialed Numbers – 6F44

- Can store up to 10 last dialed numbers
- BCD (Binary Coded Decimal) format
  - Each decimal digit is stored in a 4-bit nibble
- Most phone manufacturers do not use this feature preferring to implement this feature on the phone calling logs
  - *NOTE: SIM does not store received call data*

Speed Dial Numbers - 6F3A

- **This is the actual phone book storing contacts**
- Also called “Abbreviated Dialed Numbers”
- Up to 250 slots for storing phone numbers
- ASCII code name and BCD byte swapped number pair
- When number is deleted the slot is filled with FF hex value so deleted numbers cannot be retrieved forensically…
- However, slots are allocated in sequence
  - One can determine if a number between two numbers has been deleted

Contact name

01: 53 6B 75 6D 20 4B 6F 6E 74 61 6B 74 FF FF FF FF
FF FF FF FF FF FF FF FF 06 81 70 80 67 23 71 FF
FF FF FF FF FF FF

Public Land Mobile Network – 6F30

- Also called “Preferred Net Services”
- PLMN Consists of
  - Mobile Country Code (MCC)
  - Mobile Network Code (MNC)
  - The networks available for access
    - Up to 80 PLMN’s are stored on the SIM Card
- Forbidden PLMN – 6F7B
  - Also called “Forbidden Nets”
  - Those PLMN’s that the SIM is forbidden access
  - Up to 4 FPLMN’s are stored on the SIM Card

42 F0 70 FF FF FF FF FF FF FF FF FF

SIM protection
PIN: Personal Identification Number

- PIN locks the SIM card until correct code is entered
- Each phone network sets the PIN of SIM to a standard default number found on smart card plastics or user contract
  - Can be changed via handset
  - Protects account, even if SIM is inserted into another phone
- If PIN protection enabled, PIN will need to be entered each time the phone is switched on
- If PIN entered incorrectly 3 times in a row, SIM will be blocked requiring a PUK from network/service provider
  - Counter resets when correct PIN is entered
- PIN Code 2
  - PIN code 2 included with GSM phase II SIM cards
  - Code controls access to advanced features of phone
    - Ie. Fixed dialling list
      - A restricted list of numbers the phone can call
  - Default code is set by service provider, but editable

SIM protection
PUK: Personal Unblocking Key

- PIN entered incorrectly 3 times - SIM blocked
  - Unable to make and receive calls/SMS
- PUK needed from service provider via account or card SN
  - Usually found on smart card plastic or user contract
  - 8 Digit Code
  - Resetting PUK, resets PIN and the attempt counter
  - New PIN may be chosen
- Caution!
  - If PUK entered 10 times incorrectly, SIM is permantly disabled and the SIM must be exchanged
  - You are completely PUKed!
- PUK Code 2
  - Performs same function as the PUK, but for PIN Code 2
  - Service Provider has this code when needed

GSM SECURITY

Threats to SIM Data 1

- Knowledgeable criminals are aware of SIM properties
  - Know how to manipulate them
- Cloning SIM data for illicit use
  - Two key pieces of data
    - IMSI
    - Data Encryption Key (Ki), 128bit key shared with HLR
- IMSI can be obtained
  - From SIM using scanning software
  - Eaves-dropping on networks for unencrypted transmission of the IMSI
- Ki cannot normally be obtained directly as it is derived from the encryption algorithm stored on SIM
- http://www.gsm-security.net/

GSM SECURITY

SIM

- How mobile phones work (GSM)

BTS

Call received by nearest base station

BSC

Base station controller determines power of transmitters and manages handover of calls made from one cell to the next if you are moving

Radio access network

MSC

MSSC patches the call into the Public Telephone Network which directs call to the mobile or landline

Core network

PSTN or other PLMN

Public Telephone Network

Base station controller passes call to Mobile Services Switching Centre (MSSC)

VLR

Visitor Location Register

Requests user details from home location register. Tells network where phone is

HLR

Home Location Register

Holds all information on every user

AuC

Authentication Centre

Security checks caller ID on SIM Generates encryption key for the call

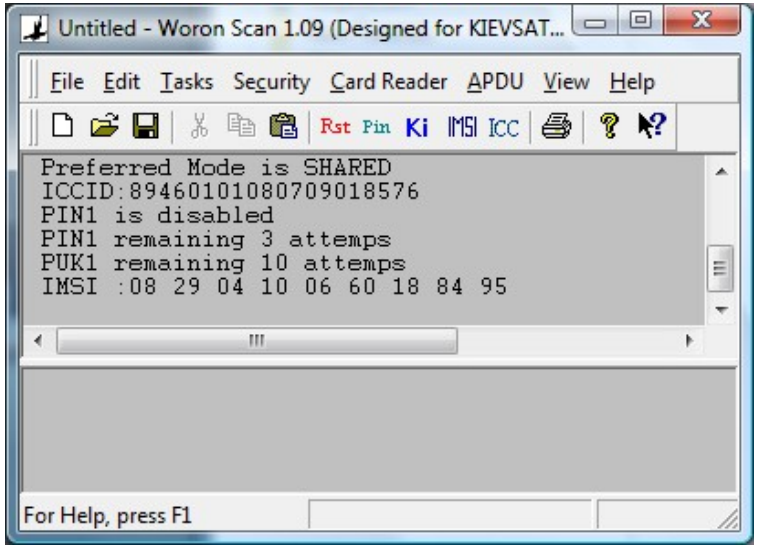
EIR

Equipment Identity Register

Requests IMEI from phone and bars call if blacklisted

Threats to SIM Data 2

- GSM SIM's can be cloned because authentication protocol has flaw
  - COMP128v1 is a popular algorithm and a published standard
    - Leaks information at every connect attempt
    - Sufficient number of challenges to SIM card produces enough info to deduce secret key
- Chosen-plaintext attack to extract Ki
  - Approximately 150000 queries required, takes about 4-8 hours with a suitable smart card reader
- http://en.wikipedia.org/wiki/SIM_cloning
- Google on "GSM SIM cloning" and "woron scan"



GSM Hacks

Threats to SIM Data 3

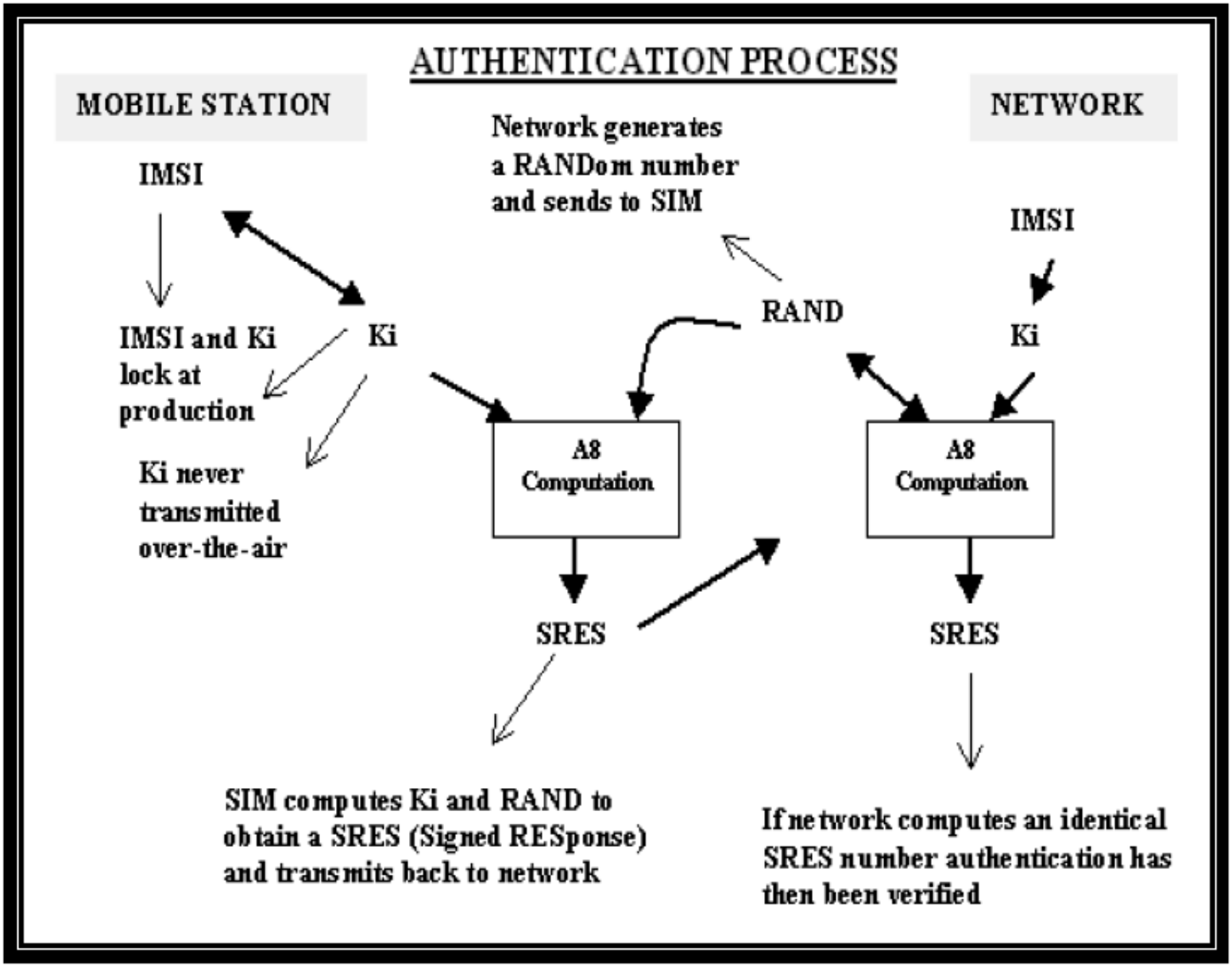
- SimScan software can obtain the Ki electronically but at the risk of damaging the SIM
  - 40% chance of damaging the card
- Obtaining blank SIMs
  - Cannot reprogram IMSI or Ki data on a SIM card obtained through any other means than direct from the manufacturer
  - MSAB SIM ID Cloner can however program IMSI and ICCID
- Security have been improved with the COMP128v2 and COMP128v3 algorithms
  - Takes time to change for the carriers since it is stored in SIM
  - http://www.gsm-security.net

GSM SECURITY

SIM Encryption - Authentication

- Most GSM providers use a version of COMP128vx (A3+A8) for both the A3 authentication algorithm and the A8 key generation algorithm
- Authentication involves two functional entities
  - The SIM Card in mobile device, and
  - The Authentication Center (AuC)
- Each subscriber is given a secret key (Ki), one copy of which is stored in the SIM card and the other in the AuC
- During authentication, AuC generates a random number that it sends to the mobile
- Both mobile and AuC use the random number, in conjunction with subscriber's secret key and a ciphering algorithm to generate a SRES (Signed RESponse) number that is sent back to the AuC
- If SRES number sent by mobile matches number calculated by AuC, then subscriber is authenticated

GSM - Authentication



Physical - Authentication

- A list of IMEIs in the network is stored in the EIR (Equipment Identity Register)
- The status returned in response to an IMEI query to the EIR is one of the following:
  - White-listed
    - Terminal is allowed to connect to the network
  - Grey-listed
    - Under observation from the network, possible problems
  - Black-listed
    - Terminal has either been reported as stolen, or it is not type approved (the correct type of terminal for a GSM network)
    - The terminal is not allowed to connect to the network
- CDMA networks have ESN instead
  - Electronic Serial Number

SIM Encryption - Key Generation

- A8 algorithm generates a 64-bit Session Key (Kc)
  - From 128-bit random challenge (RAND) received from MSC (Mobile Services Switching Center) and
  - From 128-bit Ki (Individual Subscriber Authentication Key) from Mobile Station's SIM or HLR (Home Location Register)
- One Session Key (Kc) is used until the MSC decides to authenticate the MS again - which may take days
- A8 algorithm actually generates 128 bits of output
- The last 54 bits of those 128 bits form the Session Key (Kc)
- Ten zero-bits are appended to this key before it is given as input to the A5 algorithm
- The A8 algorithm is implemented in the SIM

GSM – A5 Encryption

- The encryption algorithm used in the GSM system is a stream cipher known as the A5 algorithm
- Multiple versions with various levels of encryption
  - A5/0: no encryption
  - A5/1: original A5 algorithm used in Europe
  - A5/2: weaker encryption algorithm created for export and used in the United States
  - A5/3: strong encryption algorithm created as part of the 3rd Generation Partnership Project (3GPP)
    - Also known as the KASUMI algorithm

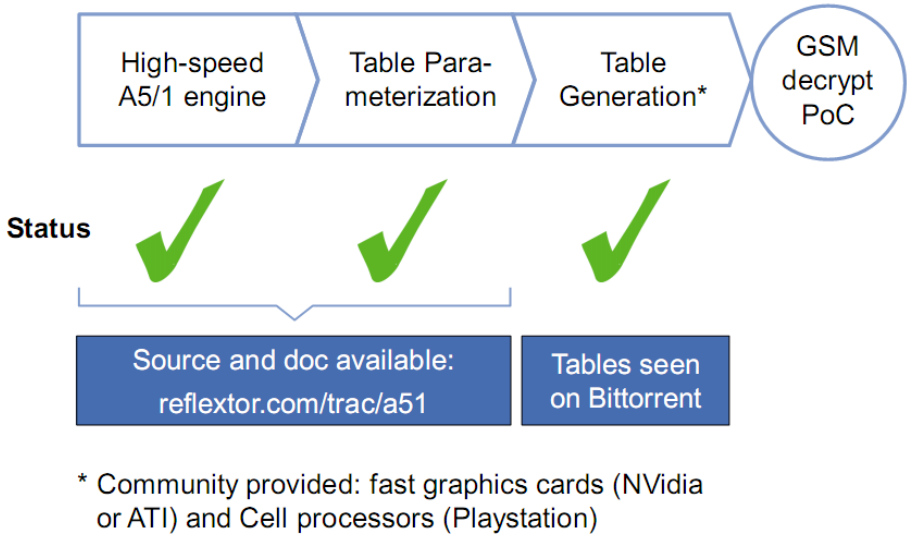
GSM - Encryption

- The stream cipher is initialized with the Session Key (Kc) and the number of each frame
  - The same Kc is used throughout the call, but the 22-bit frame number changes during the call, thus generating a unique key stream for every frame
- The same Session Key (Kc) is used as long as the Mobile Services Switching Center (MSC) does not authenticate the Mobile Station again
  - The same Session Key (Kc) may be in use for days
- Authentication is an optional procedure in the beginning of a call, but it is usually not performed
- The A5 algorithm is implemented in the Mobile Station/Equipment (MS/ME) handset
- A5/1 is constantly being academically broken but proof of concept has just recently been published

GSM SECURITY

GSM – A5/1 Cracking Project

- Karsten Nohl presented on the 26C3 conference in december 2009 how to crack the A5/1 - proof of concept shown
- Two types of attack
  - Active intercept
    - Phones connect through fake base station
  - Passive intercept
    - Key cracking
- Code book 128 Petabyte large and rainbow table generation
  - 100k years on 1 CPU
  - 3 months on 40 GPUs
- Code and presentation
  - http://reflextor.com/trac/a51
- Rainbow tables
  - http://reflextor.com/torrents/



GSM – A5/3 Cracked to!

- Two weeks after A5/1, cracked A5/3...
- Researchers Crack 3G GSM 128-bit Encryption in Under 2 Hours
  - Orr Dunkelman, Nathan Keller and Adi Shamir
  - Paper

http://www.drsuresh.net/?p=14

http://eprint.iacr.org/2010/013

Universal Subscriber Identity Module and R-UIM

- USIM is a 3G SIM card
- Differences include:
  - Greater storage capacity, > 1 GB
  - Enhanced phone book (e.g. nickname, email etc.)
  - But same physical shape and size
- Combination (hybrid) cards exist
- Removable User Identity Module (R-UIM)
  - A card developed for CDMA
  - Extension of the GSM 11.11 standard
  - Superseded by CSIM
  - http://en.wikipedia.org/wiki/R-UIM

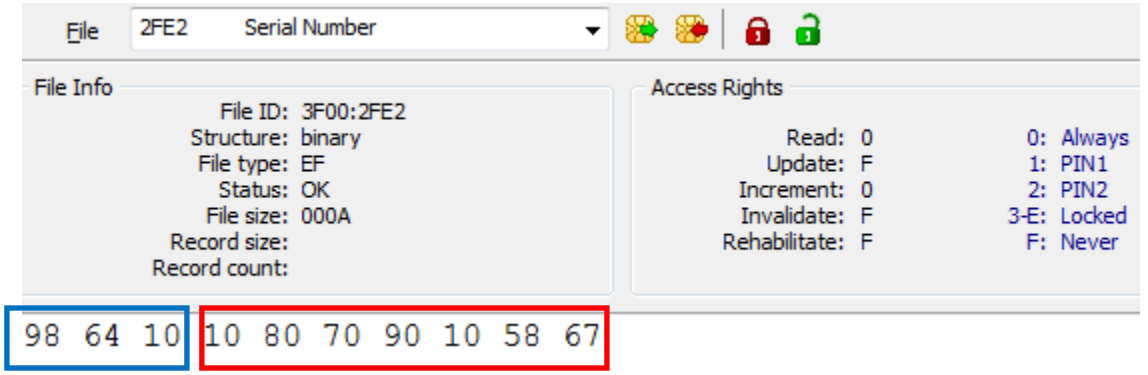
Readings

- http://www.forensicswiki.org/wiki/SIM_Cards
- Evidence in Mobile Phone Systems
  - By Svein Y. Willassen, M.Sc.
- Reading SIM and SMS the hard way ...
  - http://brokenpipe.de/misc/chipcard/sim-intro.html
- A Smart Card Framework for .NET
  - http://www.codeproject.com/KB/smart/smartcardapi.aspx
- SIMspy II and PDUspy
  - http://www.nobbi.com/download.html

Backups

Integrated Circuit Card Identifier

- **ICCID** uniquely identifies the card, one can determine issuing service provider and country from ICCID
- International Standard ISO/IEC 7812
  - http://en.wikipedia.org/wiki/ISO_7812
  - 19 or 20 digits in length and always stored in the card
  - Normally printed on the outside (may be abbreviated)
- Issuer Identification Number (IIN)
  - Major Industry Identifier (MII), 2 digits, 89 for telecommunication purposes
  - Country code, 1-3 digits, as defined by ITU-T recommendation E.164.
  - Issuer identifier 1-4 digits, (Total all 6 digits including the MII)
- Individual account identification
  - Max 12 digits plus
  - Parity check digit



International Mobile Subscriber Identity

http://en.wikipedia.org/wiki/IMSI
http://pt.com/page/tutorials/gsm-tutorial

- **IMSI** uniquely identifies a subscriber
  - Always provisioned in the phone/SIM (GSM), USIM (3G) or CSIM (CDMA)
  - Usually 15 digits in length
- Ex. IMSI: 240011234567890
  - The first 3 digits are the Mobile Country Code (MCC)
  - Followed by the Mobile Network Code (MNC)
    - Either 2 digits (EU standard) or 3 digits (North American standard)
  - The remaining digits are the Mobile Station Identification Number (MSIN)

IMSI = MCC + MNC + MSIN

MCC	240	Sweden
MNC	01	Telia
MSIN	1234567890	

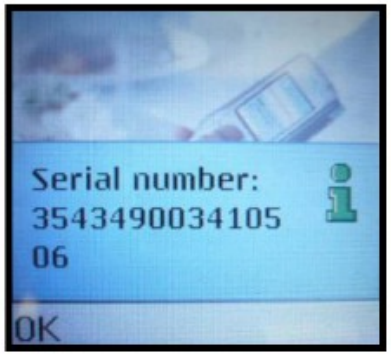
- IMSI analysis
  - The process of examining a subscriber's IMSI to identify which network the IMSI belongs to and whether subscribers from that network are allowed to use a given network

International Mobile Equipment Identifier - IMEI

http://en.wikipedia.org/wiki/IMEI

- 15 digits in length
- Stored digitally in the handset
- Printed on a sticker under the battery
- You can determine make, model and serial from IMEI
- IMEI-number 35-209900-176148-1 means:
  - **TAC** (Type Approval Code): 352099 (allocation number 2099)
  - **FAC** (Final Assembly Code): 00
  - **SNR**: 176148 - uniquely identifying a unit of this model
  - **Control Digit**: 1

The two versions *should* match...



Type *#06#

USIM
(Future Evolution of SIM Technology)

- Multi-Subscription, Multi-Application
- Java-Based USAT
  - Universal SIM Application Toolkit
- Higher Data Rates
  - Mobile Commerce
  - Mobile Music
  - Mobile Internet
  - Mobile Video Conferencing
- Full Backwards Compatibility

USIM

- 256 KB EEPROM
- 384 KB ROM
- 8 KB Static RAM
- 16-bit Calm RISC CPU
- Triple DES
  - The standard symmetrical key encryption