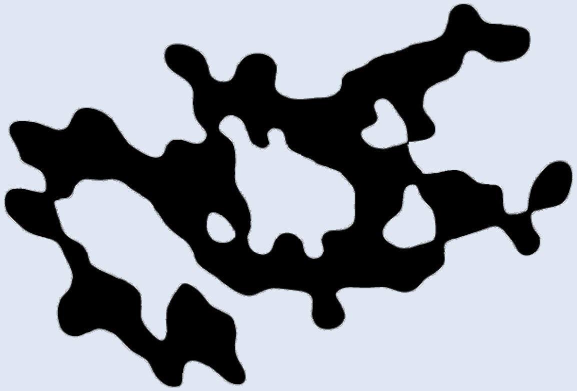
The blackbox in your phone

Hunz
Zn000h at gmail.com



CCC Camp 2011
10.08.2011

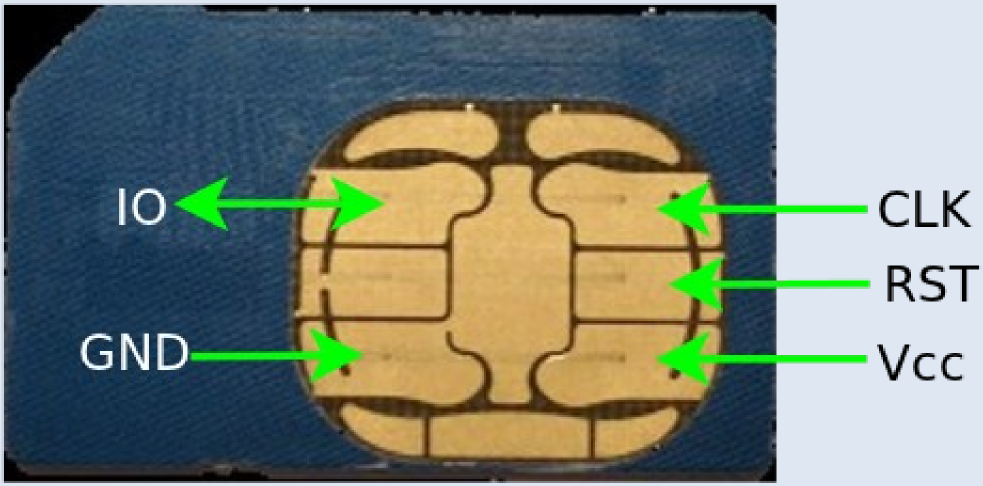
Contents

- Smartcards in general
- The SIM
  - filesystem
  - commands
- SIM application toolkit (SAT)
- Tools
- Summary

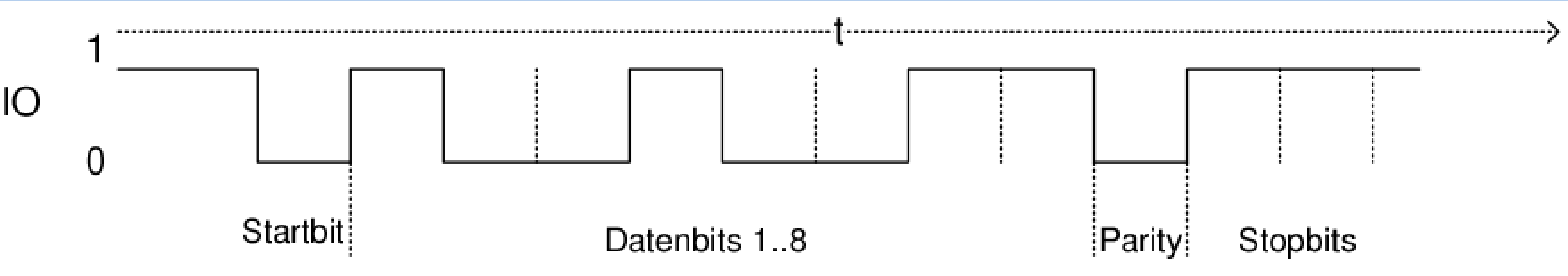
Smartcards: physical connections

- Not just memory, but a microcontroller → card decides, what the user can do

- Connections:
  - RST: Reset input
  - CLK: Clock input
  - IO: Data in/out
  - Vcc: supply voltage (1.8V / 3V)

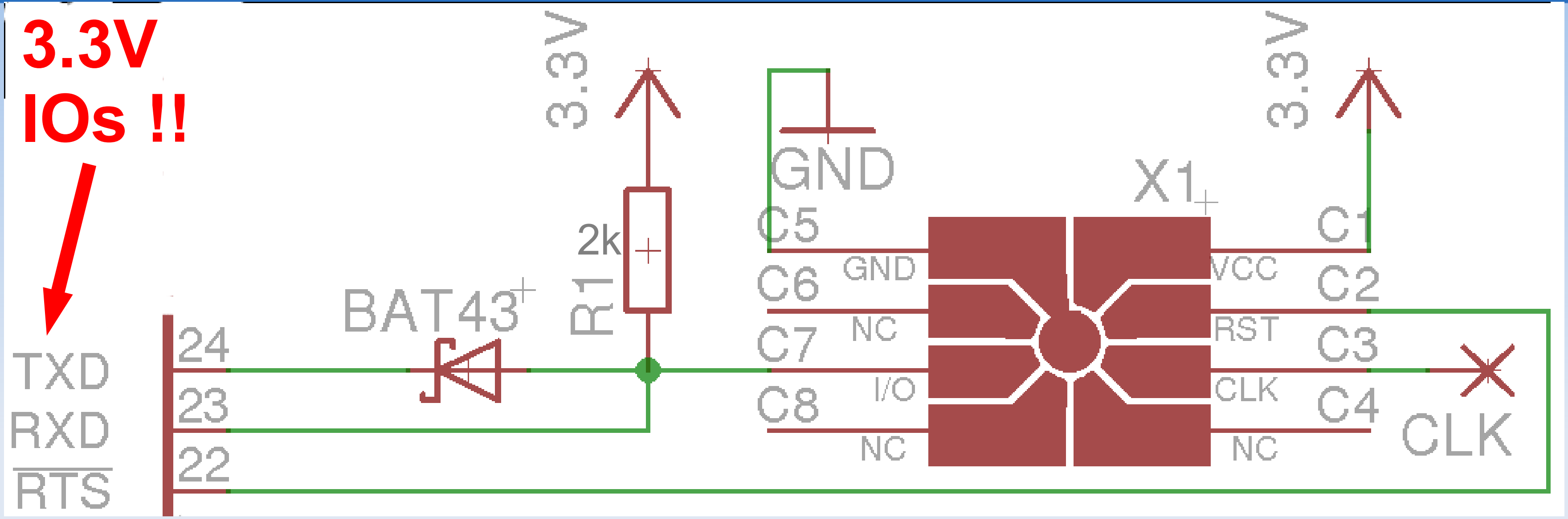


Smartcards: data transmissions



- Serial protocol like RS-232
- But: only one data line → half duplex
- Request/response with Terminal as Master
- Baudrate depends on input clock
  - Initial baudrate = clk / 372

A simple smartcard terminal



3.3V
IOs !!

- Phoenix & Smart-/Dumbmouse Terminals
- RS-232 UART used for communication
    - Card clock = 9600 baud * 372 = 3.5712 MHz
    - IO: Open collector w/ pullup
- RTS used for card reset (polarity may vary)
- Or: use a PC/SC reader

Smartcards: Protocol setup

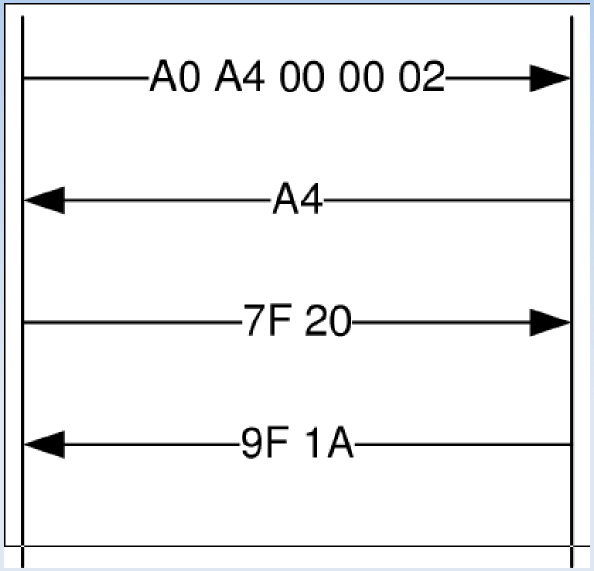
- Card reset
- Card sends Answer-to-Reset (ATR)
  - Supported parameters, protocols, etc.
  - ATR: 3B <more stuff>
  - Decode w/ pcsc_tools: ATR_analysis
- Protocol-Parameter-Selection (PPS)
  - protocol+baudrate selection
  - optional, but heavily used nowadays

Smartcards: T=0 Protocol

CLA	INS	P1	P2	Len	(Data)	SW1	SW2
Terminal → Card					To or from card	Card → Terminal	

- Communication via Application Protocol Data Units (APDU)
    - CLA: Instruction Class
    - INS: Instruction (command)
    - P1, P2: Instruction-specific parameters
    - Len: Data length
    - Data (optional) either to or from card
    - SW1, SW2: Status (from card)

Smartcards: T=0 Example



1) ADPU Header (Terminal → Card)

2) ACK (Card → Terminal)

3) Data (Terminal → Card)

4) Status (Card → Terminal)

- Card sends ACK/INS (or error-status) after data length received

Smartcards: Further reading

- ISO/IEC 7816: http://en.wikipedia.org/wiki/ISO/IEC_7816
- Smartcard handbook:

  http://www.wrankl.de/SCH/SCH.html
- Handbuch der Chipkarten (german): http://www.wrankl.de/HdC/HdC.html
- Phoenix reader – you can build your own
  - Several designs → use google
  - Replace MAX232 w/ FT232 or so for USB
  - Use 3.3V instead of 5V!

Purpose of the SIM

- User authentication
- Network authentication (3G)
- Data storage (phonebook, SMS, settings)
- Common platform for additional services

  → SIM Application Toolkit

SIM filesystem

- Access control
- Contains directories & files
  - identified by 16bit File-ID (FID)
  - MF (Master File) : root dir (FID: 3f00)
  - DF (Dedicated File) : directory
  - EF (Elementary File) : file
- Special EF types: record files
  - Fixed or variable length Example: Phonebook
  - Cyclic Example: Call History

SIM filesystem: important FIDs

- DF_GSM: Network related data FID: 7F20
  - EF_IMSI: IMSI FID: 6F07
  - EF_Kc: session key FID: 6F20
  - Etc.
- DF_TELECOM: Data for user FID: 7F10
  - EF_SMS: SMS storage FID: 6F3A
  - EF_ADN: phonebook FID: 6F3C
  - Etc.

SIM filesystem: a few notes

- SELECT instruction opens a file for access
- FIDs usually aren't unique across directories
  - Different EFs in different DFs may have same FID

  → SELECT needs to follow path of directories

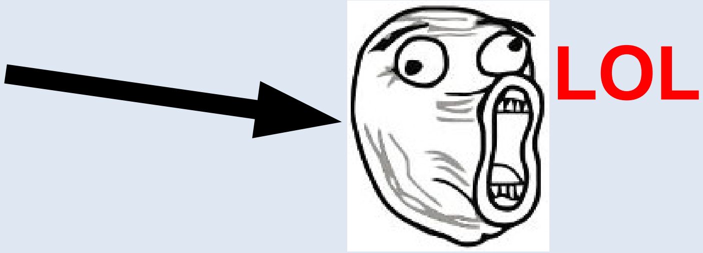
  - Example: SELECT MF; SELECT DF_GSM; SELECT EF_IMSI

- There's no directory listing like “ls”
  - FIDs for GSM are published in the specs
  - Are there any hidden (non-specified) FIDs?

Tool: SIM_dump

- Phoenix only, no PC/SC yet
- Bruteforce-approach on FIDs

  → find hidden files
- C-tool to dump files from SIMs - no USIMs yet
  - Quick, ugly hack. Stable?
  - But I tested it once!1



- Still want the code?

  → https://github.com/znuh/simdump

SIM instructions (1)

- 1 APDU can only transfer data to or from card
  - What if we need both?
  - GET_RESPONSE fetches the answer

A0	**C0**	0	0	Len	Data	SW1	SW2

- How to select a FID?
  - SELECT

A0	**A4**	0	0	2	**FID**	SW1	SW2

- Read/update/etc. File
  - Would bloat this talk too much

SIM commands (2)

- RUN GSM
  - User authentication
  - Session key (Ciphering Key (Kc)) generation

A0	**88**	0	0	16	**Random value from net**	SW1	SW2

  - Answer via GET RESPONSE:

A0	**C0**	0	0	12	**SRES(4) + Kc(8)**	SW1	SW2

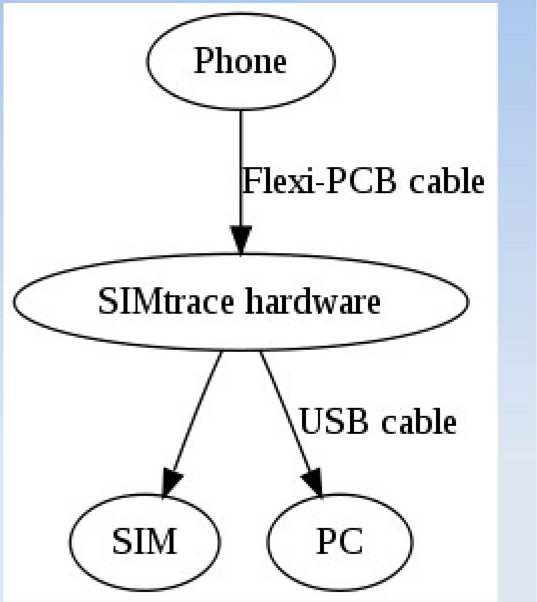
  - SRES: Authentication response
  - Kc: Ciphering key

USIMs

- Backwards compatible
- Multiple Applications on a single card
  - EF_DIR (2F00) has a list of installed applications
  - Application ID (AID) selection
- Other CLA for USIM – 00 instead of A0
- Mutual (network & user) authentication
  - AUTHENTICATE instruction
  - Details: http://tools.ietf.org/html/rfc3310

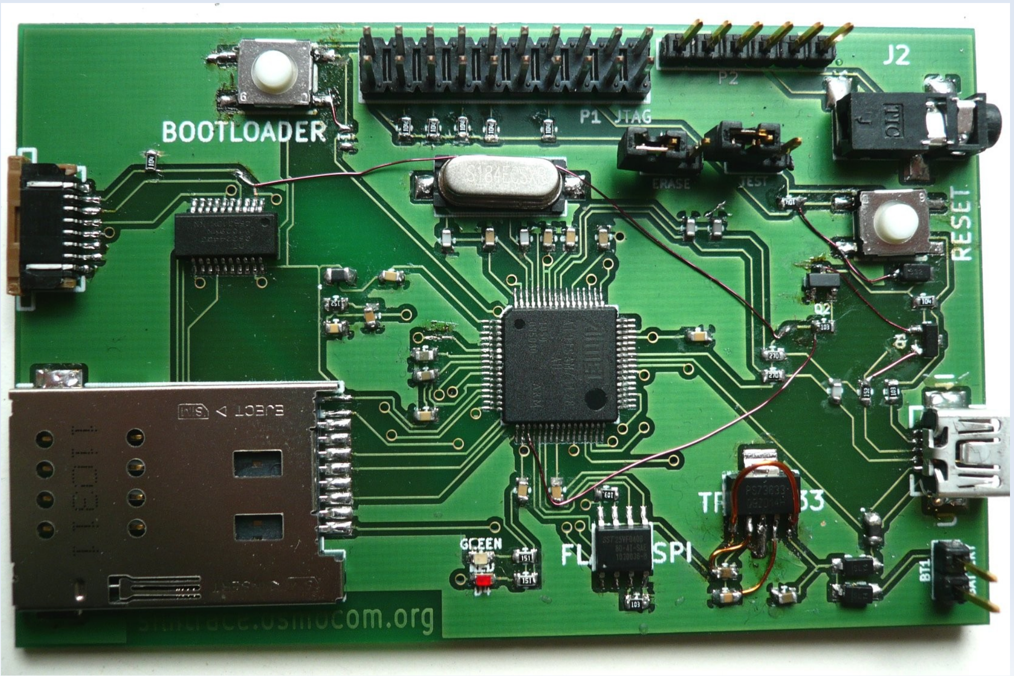
Tool: SIMtrace

- Hardware sniffer for phone ↔ SIM
- With inject support! → MITM
- Made by the osmocom guys



- Cheap AND open

- Get it here at the camp
- There's a workshop
- See RadioVillage



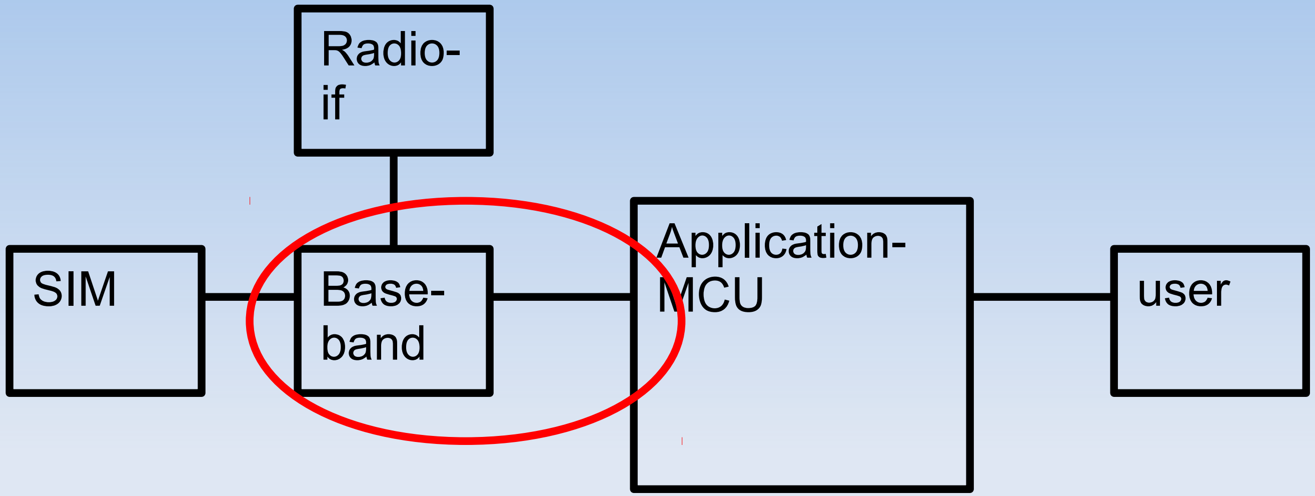
Tool: SIMtrace

```
Example:
APDU: (22):   a0 c0 00 00 0f
              00 00 00 09 6f 38 04 00
              15 00 55 01 02 00 00
              91 78
APDU: (16):   a0 b0 00 00 09
              ff 3f ff ff 00 00 3f 03
              00
              91 78
```

The SIM Application Toolkit (SAT)

- Normal way: phone sends commands to SIM
- SAT: Commands from SIM to phone
- Why?
  - Additional phone-independent services
- How?
  - Terminal is master → polling
  - New instructions, status word (91xx instead of 9000)
  - SAT Commands part of GSM/3G spec

SAT architecture (phone-side)



- Most stuff is done in baseband!
- App-MCU mostly for user-interaction

SAT instructions

- Terminal profile (data: phone → SIM)

A0	**10**	0	0	Len	Data	SW1	SW2

  - Notify SIM about SAT-features supported by phone

- Fetch (data: SIM → phone)

A0	**12**	0	0	Len	Data	SW1	SW2

  - Fetch SAT commands from SIM

SAT instructions (2)

- Terminal response (data: phone → SIM)

A0	**14**	0	0	Len	Data	SW1	SW2

  - Answer to SAT-commands from previous Fetch

- Envelope (data: phone → SIM)

A0	**C2**	0	0	Len	Data	SW1	SW2

  - Notify SIM about some event
  - Example: menu selection, SMS received, call setup

SAT commands

- Transmitted in data-part of Fetch-instruction
- Some interesting features:
  - Set up call & call control
  - Send short message
  - Run AT command
  - Data channel stuff
  - Provide local information (cell IDs, signal levels)
  - Geographical Location Request (yes, that's GPS)

SAT command encoding

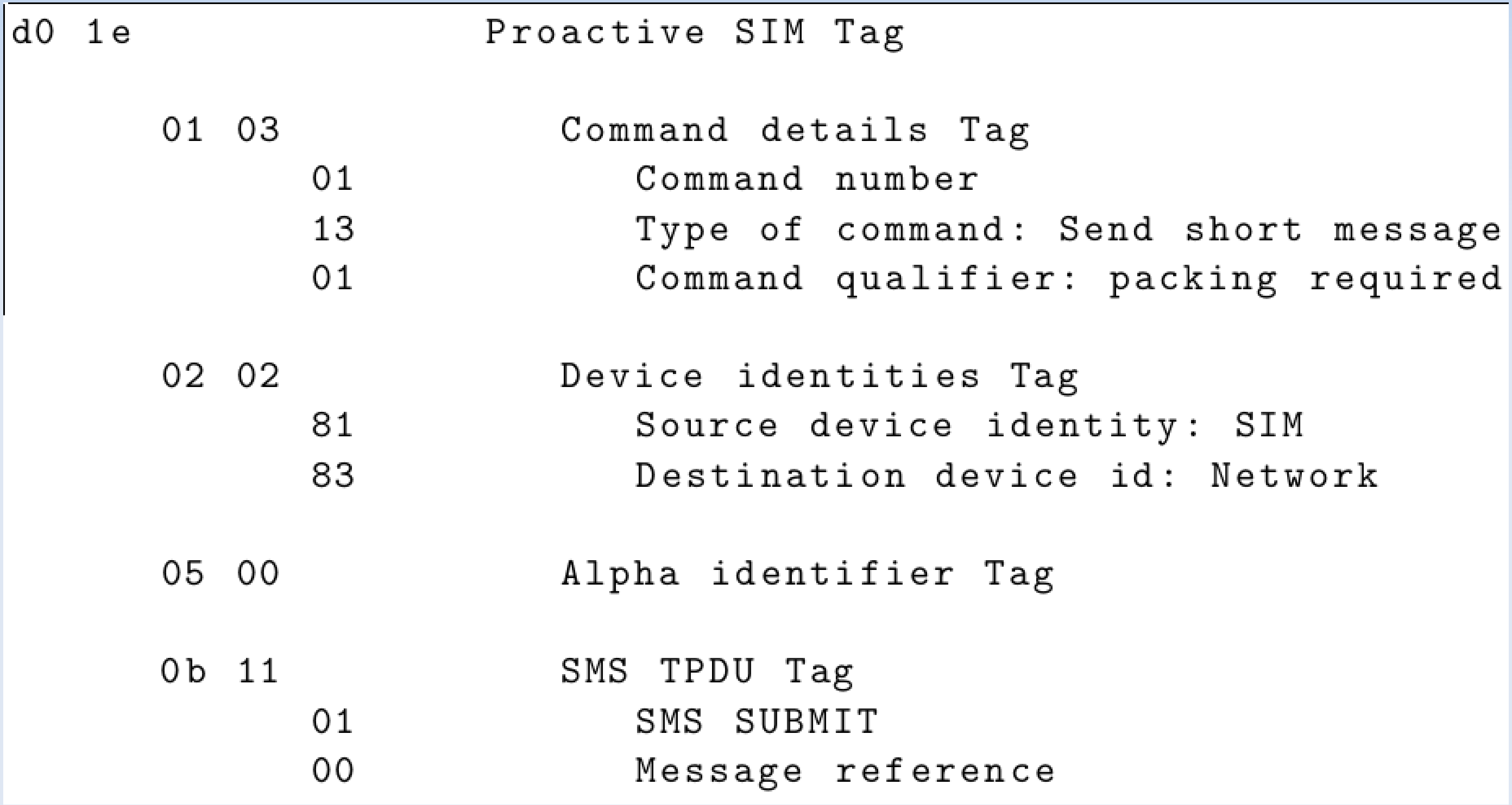
Commands + parameters are TLV encoded:

- Proactive SIM tag
    - Command details tag
        - Actual command
    - Other Parameters ...
        - …

- Mandatory and optional parameters
- Alpha identifier tag controls notification of user

SAT example: send SMS

- Fetch data:



```
d0 1e                Proactive SIM Tag

        01 03               Command details Tag
                01              Command number
                13              Type of command: Send short message
                01              Command qualifier: packing required

        02 02               Device identities Tag
                81              Source device identity: SIM
                83              Destination device id: Network

        05 00               Alpha identifier Tag

        0b 11               SMS TPDU Tag
                01              SMS SUBMIT
                00              Message reference
```

...

Over-the-air update

- SMS-PP download via Envelope instruction
- Like “silent SMS”, but sent to SIM card
- Usually, there's crypto (DES/RSA?) for this
- Haven't had a closer look at this
- A virgin SIM might be a good start for this

Further reading (SIM-related)

- ETSI TS 102 221: SIM instructions, etc.
- 3GPP TS 31.102: SIM files, procedures
- 3GPP TS 31.111: SIM application toolkit
- There's a lot more

- Useful tool for SMS de/encoding: PDUspy
- Session-logs from real (U)SIMs

Summary

- SIM features:
  - phone control via SAT (calls, SMS, data, etc.)
  - location tracking
  - remote updates
- You don't know what the SIM firmware does
- With most mobile phones you cannot
  - disable the SAT
  - or see what the SAT actually does
- 3GPP SAT spec is growing (new features!11)

So what can be done?

- Watch 3GPP specs for new features
- Patches for phones (Problem: → baseband?)
  - SAT filter
  - SAT monitoring
- Which SAT-features do phones support?

  → SIMtrace
- Which SAT-features are actually used?
  - Operator specific
  - Needs long-term monitoring

- Thanks for your attention!