osmocom SAP branch

Nico Golde, Kevin Redon

nico@ngolde.de, kevredon@mail.tsaitgaist.info

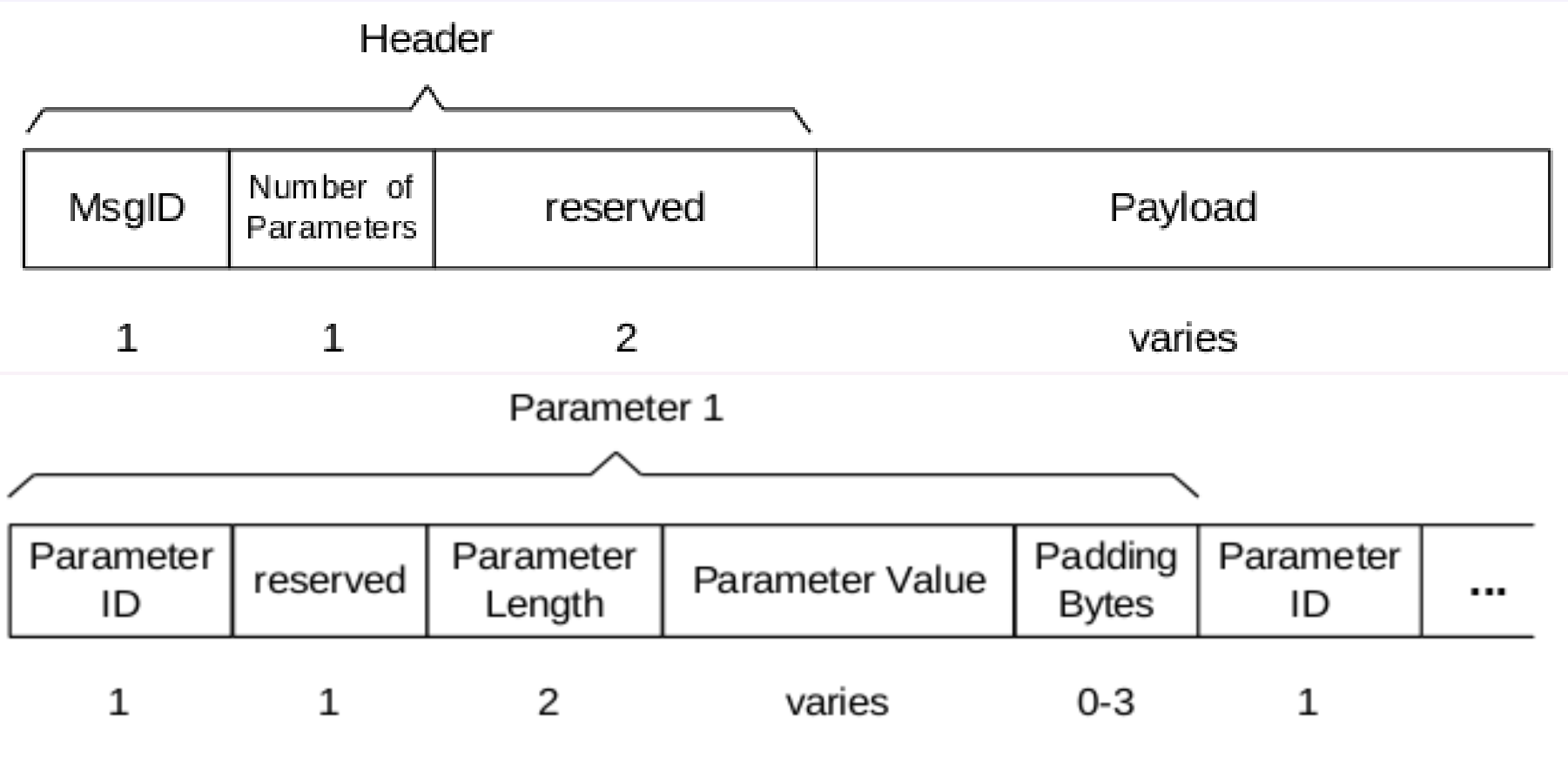
June 27, 2012

- **S**im **A**ccess **P**rofile has been adopted as Bluetooth profile
- Designed to be used in cars
  - Car acts as a faraday cage
  - High end cars have good antennas and feature GSM modems
    $\rightarrow$ utilize car modem rather than phone modem
- Car modem communicates to phone SIM over BT
- SAP has no hard requirement for BT

- Our motivation: remote SIM access/SIM card emulation [1]
- Other motivations:
  - standardized SIM interface between layer23/layer1(osmocon)
    $\rightarrow$ remote SIM access
    $\rightarrow$ using osmocom as SIM reader with osmocon as SAP server

[1] http://bb.osmocom.org/trac/wiki/softSIM

- SAP is fairly simple



- Basically wraps APDUs and provides some management messages
- Simple state machine (basically idle or processing)
- SAP provides message types (request/response) to:
  - connect/disconnect
  - transfer APDU/ATR
  - SIM power off/on
  - error handling, ...
- We currently only send atr, connect, apdu, disconnect

- Currently only the layer23 client exists and needs testing!
- l1ctl.c (l1ctl_tx_sim_req) routes APDUs to SAP client or layer1
- Communicates over SAP unix domain socket (/tmp/osmocom_sap, config-mode sap-socket PATH)
- Server is part of softSIM repository and uses PCSC

DEMO

Useful Information

- src/host/layer23/
  - src/common/sap_interface.c
  - include/osmocom/bb/common/sap_interface.h
- git branch: remotes/origin/nion/sap
- `https://www.bluetooth.org/DocMan/handlers/DownloadDoc.ashx?doc_id=158740`
- `http://bb.osmocom.org/trac/wiki/softSIM`