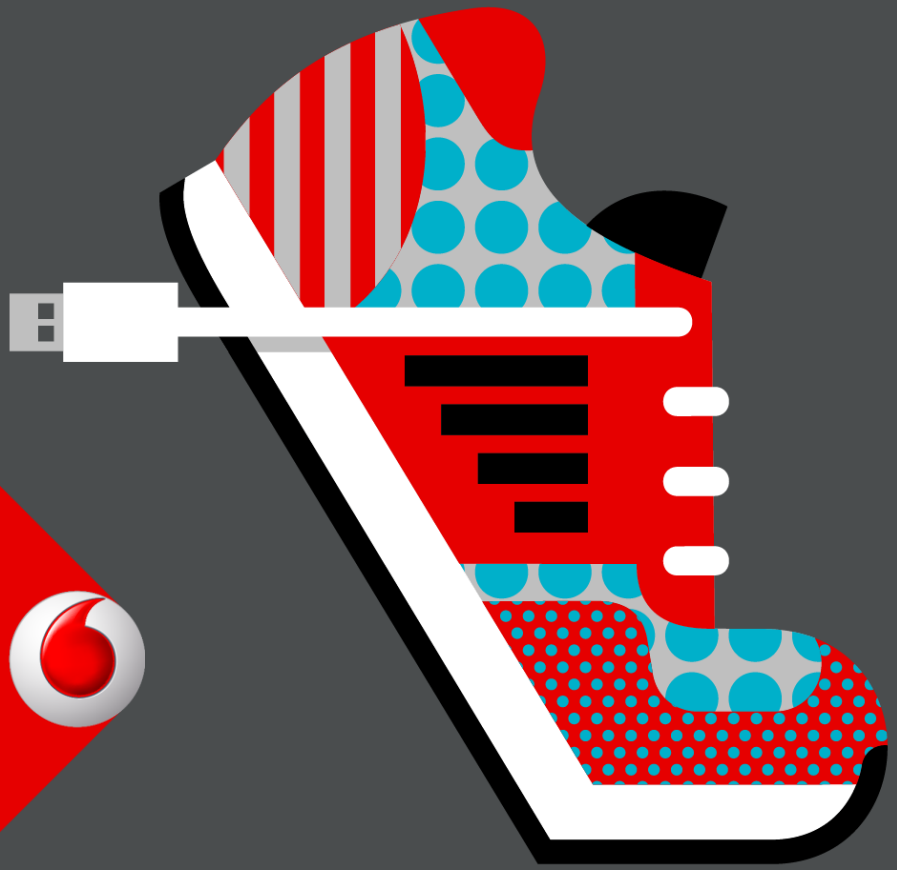
3GPP TSG SA#67,
Shanghai, 11-13/3/2015

Tdoc SP-150131

Agenda item: 5.3



GERAN Cellular Internet of Things & interactions with SA

09/03/2015
Vodafone

Overview of our requirements/targets for GERAN CIoT

- Almost perfect coverage:
  - 20 dB coverage extension over GPRS
  - reuse existing grid of base station towers and masthead equipment
- 10 year battery life on 2*AA
  - e.g. 20 bytes of information reported every 2-24 hours
- Device cost below GSM
- Use licensed spectrum
- Be secure
- Mobile Terminating services supported

- Fast to market

Background information

- PS domain only
  - no CS domain support
- SMS supported
  - e.g. to permit operator reconfiguration of preferred PLMN roaming list
  - SGSNs can support SMS, but today MO-SMS generally not configured in SGSN
- Use capabilities of Multi-Standard Radio technology (MSR permits tower-top amplifiers to be common for GSM, UMTS and LTE)
- Intra RAT mobility only by cell reselection
- Inter RAT mobility not supported (both connected and idle mode).
- Gb interface does not require a BSC in between SGSN and BTS site
- S1 interface can run to an "eNodeB" that serves many base station sites.

Some use cases

- any form of sensor or actuator with low data rate (e.g. <160 bit/s)
- Street lights (e.g. report when bulb has failed)
- Smoke Detector (e.g. weekly report to landlord that it is still working)
- Door/window open/closed status report (e.g. kids left fridge door open *again*)
- Remote controlled door locking
- Parcel tracking; pet tracking; stolen car/bicycle locator;
- Road temperature/ice sensors

Anticipate manufacturer to install SIM and later sell in multiple countries

→ Many **permanently roaming** stationary **devices**

Architecture (1)

- "Gb based" -> 24.008 NAS protocol; USIM; 44.064/44.065 User plane; 48.018 BSSGP
- "S1 based" -> 24.301 NAS protocol; USIM; GTP-U User plane; 36.413 RANAP
- New architecture?
  - infeasible to agree design and specify in R13 standards timeframe.
  - future upgrades possible (c.f. Frame Relay to "Gb over IP", ATM to "Iu over IP")

→ use an existing 3GPP Core Network

- Gb vs Iu vs S1
  - Iu rejected
  - Gb good for "one report packet and its server level ack"
  - S1 is connection oriented,
- Gb selected for "evolved GSM"
- active Gb vs S1 debate for "clean slate" approaches

Architecture (2)

- Currently no essential architectural changes yet identified for Gb based architecture
  - but SA3 input pending
- Optimisations might be useful:
  - For paging with R13 Extended Coverage LTE, RAN 1 has sent LS in S2-150019.
    LS exchange ongoing, and solutions could be made common for CIoT.

  - Reduced complexity ("profiled") GMM/EMM and SM/ESM ?

CIoT Security: paraphrasing G2 questions to SA3

- Can Gb be used or is S1 essential for security reasons?
- Can 3GPP security be done in a more appropriate manner for CIoT?

CIoT Security:
Can Gb be used or is S1 essential?

- Investigations (e.g. checks of UE log files) show that UMTS AKA is frequently used on 2G GPRS
- GEA4 (similar to UMTS security) could be mandated
  as existing devices will not be able to use new interface

- regional requirements (?) to turn off encryption may imply a need for NAS signalling integrity protection.

More appropriate security for CIoT?
- background

- Most professional M2M enterprises use end to end security (i.e. security from device to enterprise) as
  - 2G coverage may be encountered
  - no certainty that VPLMN will encrypt with strong algorithm
  - HPLMN <–> VPLMN link
- Current OTT security mechanisms seem to refresh keys frequently.
  - seems to involve 100's/1000's of bytes of data exchange
  - OK for normal "high bandwidth" 2G/3G/4G
  - but not acceptable for CIoT
    - 10 yr battery @ GPRS+20 dB limits to 20-80 bytes of data every 2-24 hours

More appropriate security for CIoT?
-> work for SA 3?

- Investigate whether suitable OTT security solutions exist for CIoT
- Investigate whether device to GGSN security is an alternative e.g. integrity protection of user plane data
- Solutions likely to be also applicable to R13 Extended Coverage LTE.

Way Forward

- Revise/agree SA3 Study Item
  - last version in SA3 was S3-151160
  - draft of an update SID is in SP-150132

- Discuss any SA2 activities.

Thank You