TD S3z(01)0042
Agenda item 3

GERAN security ~ WI status

Joint TSG SA WG 3 / TSG GERAN meeting

Madrid, 27th April 2001

José Luis Carrizo Martínez, Vodafone

Contents

- Introduction
- Status
- Open issues
- Expectations from this meeting

Introduction

- GERAN R5
  - Iu mode: alignment to UTRAN
  - Enhanced security
    - Enhanced ciphering
    - Integrity protection
- Over the last months: integrity protection
  - Some work within TSG GERAN
  - Some LSs to and from SA3
  - Some idea of the implications
  - And now we are stuck...!
    - …hence this meeting

Status

- General
  - Vague requirements
  - Stage 2 contents: ciphering covered in TS 43.051
- Ciphering
  - No progress over last meetings; near completion ?
- Integrity protection
  - RRC v RLC/MAC
  - Look into feasibility
  - Glance at implications
- Other

Open issues

- General
- Ciphering
- Integrity protection
- Other
  - LCS
  - Use of the Iur-g interface

Open issues: **general**

- Requirements
  - SA3's
  - Operators'
- Stage 2
  - Responsibility, SA3 or GERAN? I.e. 43.051 or 33.102?
  - Stage 2 for integrity protection and other issues to be created

Open issues: **ciphering**

- TS 43.051 currently contains a clause on ciphering
  - SA3 should confirm it (*adopt it)
  - There are two *FFS*s:
    - Is the RB Id contained in the RLC PDU?
    - What ‘counter’ is to be used in RLC transparent mode?
      - TDMA frame number, as in GSM
      - HFN, as in UTRAN (*and as in RLC non-transparent mode)
- RLC/MAC control messages cannot be ciphered
  - IEs are read by other MSs

Open issues: **integrity protection**

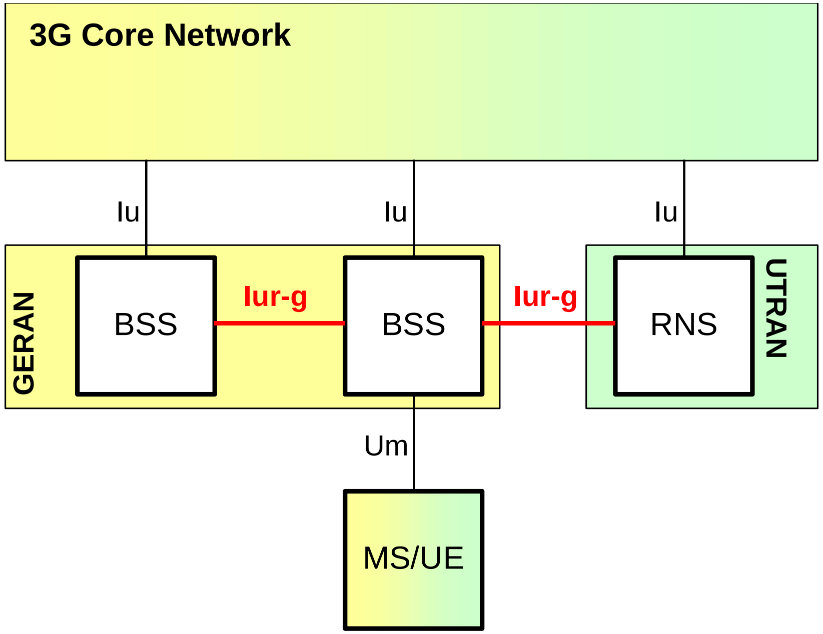
- General
  - Requirements
- Confirmation of excluded messages
- Reduction of impact on system performance
  - Shorter MAC-I
- Applicability to RLC/MAC
  - RRC-like messages / ‘all’
  - Size / frequency of messages
  - Enhancements to segmentation, especially uplink

Open issues: **other**

- LCS
  - Architectural issues still to be solved
- Use of the Iur-g interface
  - Background and working assumptions
  - Open issues

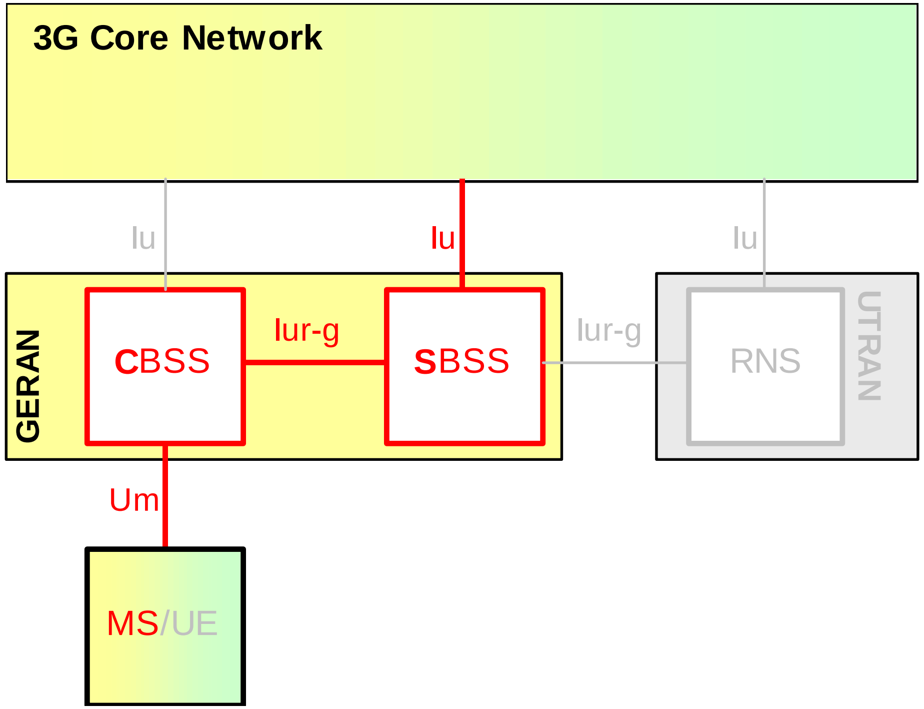
Open issues: use of the Iurg interface (i)

- Background and working assumptions
  - Between BSCs
  - Between a BSC and a RNC
  - Control plane only
  - Cell update => relocation
  - URA/GRA update ≠> relocation
    - MS(/UE) @ CBSC+SBSC
    - MS/UE @ CRNC+SBSC
    - MS/UE @ CBSC+SRNC



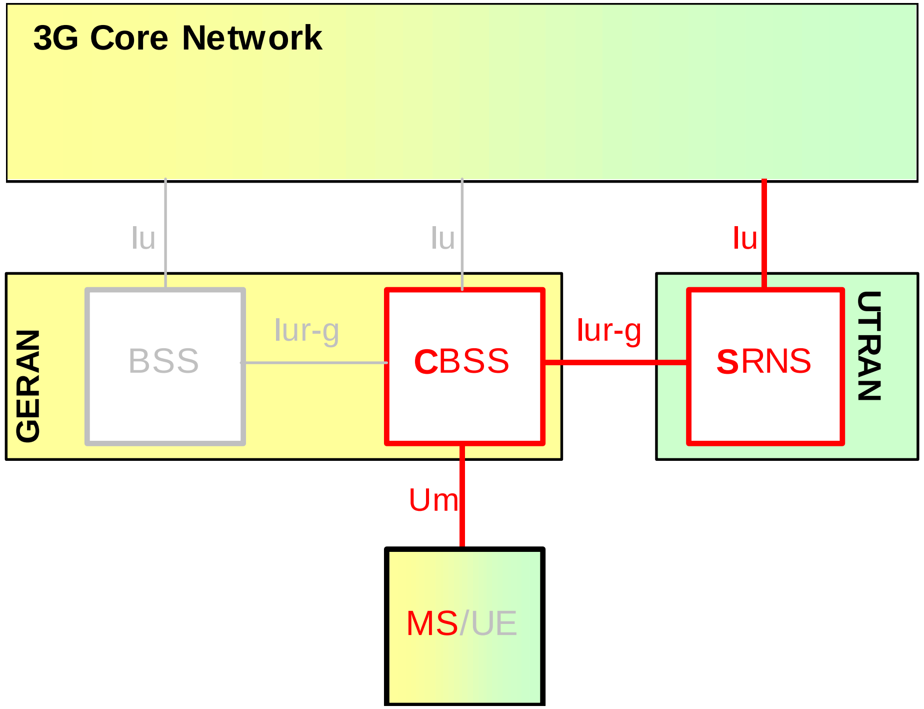
Open issues: use of the Iurg interface (ii)

- ➔ MS(/UE) @ CBSC+SBSC
- ● MS/UE @ CRNC+SBSC
- ● MS/UE @ CBSC+SRNC



Open issues: use of the Iurg interface (iii)

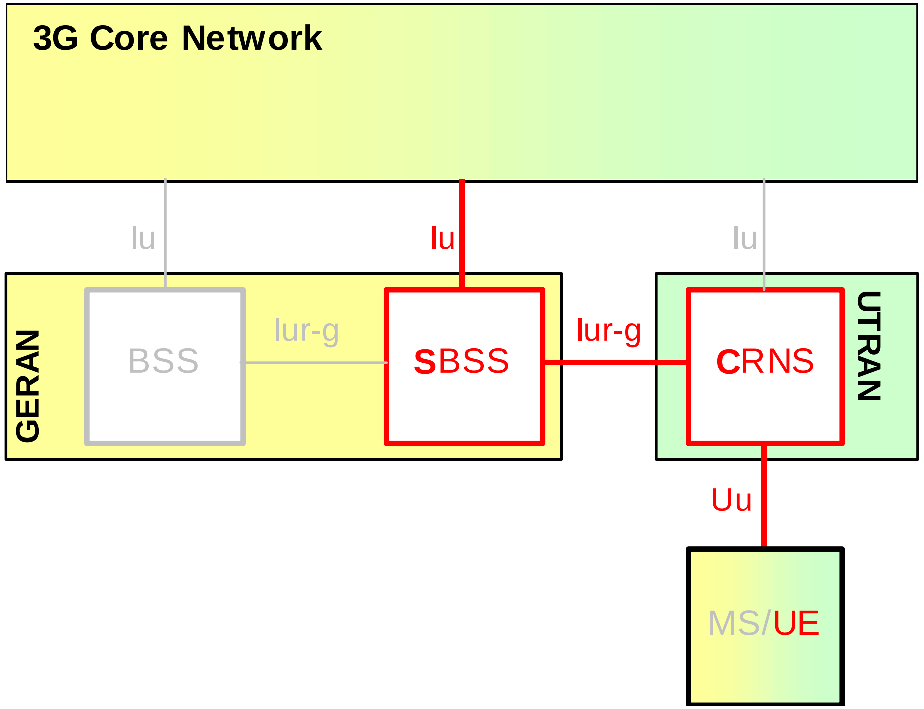
- MS(/UE) @ CBSC+SBSC
- ➔ MS/UE @ CRNC+SBSC
- MS/UE @ CBSC+SRNC



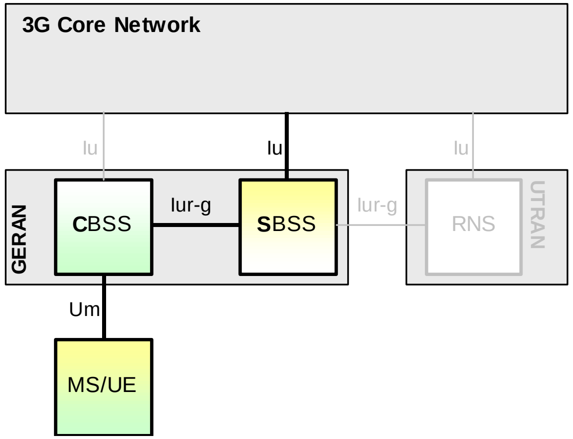
Open issues: use of the Iurg interface (iv)

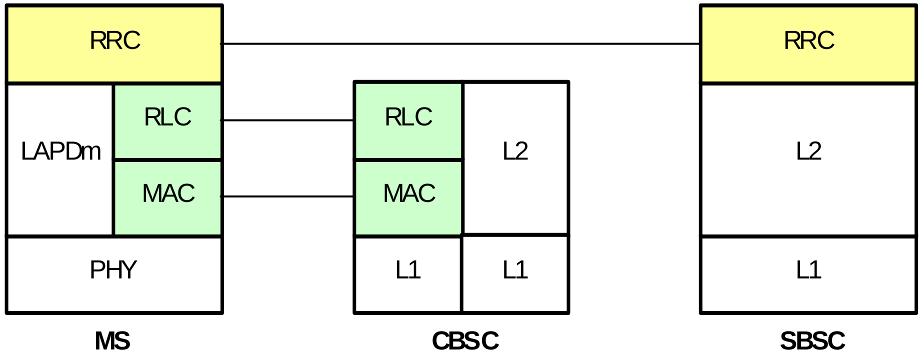
- MS(/UE) @ CBSC+SBSC
- MS/UE @ CRNC+SBSC

➔ MS/UE @ CBSC+SRNC



Open issues: use of the Iurg interface (v)





- In this scenario(s)
  - Radio resources allocated by the controlling node
  - Security terminated at the serving node
- Security implications to be studied
  - E.g. RRC procedure on a TBF

Expectations from this meeting

- Clarification of requirements
- Completion of ciphering
  - Production of CR to stage 2
- Progress integrity protection
  - Set of working assumptions
- Progress other issues
  - E.g. use of the Iur-g
- Summary:
  - CR(s) to stage 2
  - Working assumptions
  - Open issues

[redacted]