

8 – 11 October 2002**Munich, Germany**

Source: Nokia**Title: Security need evaluation of UTRAN and GERAN IP transport interfaces****Document for: Discussion and approval****Agenda Item: 7.2**

1. INTRODUCTION

This paper is related to the discussion paper *S3-020359, Security solution for UTRAN IP transport*, presented in SA3#24. The mentioned discussion paper proposed the enhancement of NDS/IP specification to cover also the control plane of UTRAN IP transport.

This study evaluates in high level the need for security protection of the IP based control plane protocols over Iu [1], Iur [2], Iub [3], Iupc [4] and Gb [5] in UTRAN and GERAN interfaces as agreed in the approved NDS/IP Rel6 WID (S3-020422). Additionally Iu-BC (between RNC and Cell Broadcasting Center/CBC) [6] and Iur-g (between RNC and BSC) [7] are covered, since they can be categorized as UTRAN/GERAN interfaces also.

The control plane in question is used to transfer signalling messages in UTRAN/GERAN IP transport network. Based on the known security threats in IP networking, the traffic needs to be protected properly. This is in order not to restrict the application of IP in UTRAN and GERAN only to closed network environments.

2. DISCUSSION

The security solution for IP based UTRAN/GERAN transport (control plane) can follow the principles introduced in the NDS/IP since the IPSec provides application independent security solution for all IP traffic.

Iu interface is carrying information that can be classified as most sensitive. Iu is used for conveying e.g. security keys. These keys are vital for the end-user security. Hence Iu is proposed to be encrypted along with the integrity check.

For Iub and Iur interfaces the lower priority proposal is to have integrity checking. This is needed because of the sensitive nature of signalling messages – it needs to be checked that the messages are coming from the correct source and that they have not been altered. Iub and Iur do not transfer security related keys or other so critical information and the encryption is not the required feature there. Iur only transports the key identifier value (KSI), but not the key itself.

Iupc is used for conveying location related data. This information is sensitive especially from the UE's point of view and for guaranteeing that no unauthorized changes are made, this interface should be integrity checked. However, encryption is not needed, as there traverses only location information

without any UE/subscriber information. Only transaction IDs are used between RNC and SMLC.

Gb integrity checking is not critical because end-user keys are not transferred over Gb; encryption is done in SGSN.

There exists also lu-BC and lur-g interfaces in UTRAN/GERAN as stated in the introduction. Regarding the nature of lu-BC traffic encryption is not seen very beneficial for it and it is thus proposed to be integrity checked. lur-g falls under same category as lur, so integrity check is recommended, since it is inter-NE signalling and not confidential subscriber information.

3. CONCLUSION AND PROPOSAL

As a conclusion, the recommendation is to have encryption and integrity protection on lu interface. Lower priority proposal is to use integrity checking for control plane interfaces that are IP based, which are namely lur, lub, lupc, lur-g and lu-BC. Gb interface is already covered by encryption in SGSN, so it does not need NDS/IP mechanism to be secure.

TS 33.210 NDS/IP likely does not need so dramatic changes, since the considered interfaces are Zb interfaces according to 33.210 notation. However, some protocol profiling is likely to be needed as the control plane of UTRAN/GERAN IP transport includes different protocol stacks than the core network, and for example SCTP is used widely in UTRAN. Additionally it has to be studied more closely if some interfaces can be classified as the inter-domain Za interface.

References:

- [1] 3GPP TS 25.412 UTRAN lu interface signalling transport
- [2] 3GPP TS 25.422 UTRAN lur interface signalling transport
- [3] 3GPP TS 25.432 UTRAN lub interface: signalling transport
- [4] 3GPP TS 25.452 UTRAN lupc interface signalling transport
- [5] 3GPP TS General Packet Radio Service (GPRS); Base Station System (BSS) - Serving GPRS Support Node (SGSN) interface; Gb Interface Layer 1
- [6] 3GPP TS 25.419 UTRAN lu-BC interface: Service Area Broadcast Protocol (SABP)
- [7] 3GPP TS 43.930 lur-g interface, Stage-2