3GPP TSG SA WG3 Security — S3#26 **S3-020692**

19-22 November, 2002

Oxford, UK

Work Item Description

Source SA3

Title GERAN A/Gb mode security enhancements

1 3GPP Work Area

X	Radio Access
X	Core Network
	Services

2 Linked work items

None.

3 Background

The GERAN Release 5 specifications support Iu mode, which enables the connection of a GERAN BSC to a 3G MSC and 3G SGSN via the same Iu interfaces as used by the UMTS RNC. Among other things, Iu mode allows IMS services to be offered over GERAN access networks. GERAN Iu mode also offers an enhanced level of security compared to 2G GSM. The level of security achieved is comparable to UMTS.

4 Justification

GERAN is currently investigating the possibility to evolve the 2G interfaces and protocols. In particular, they are studying the support of streaming IMS services over an enhanced Gb interface between the BSC and the SGSN. The work in GERAN to upgrade the existing 2G interfaces to support streaming services assumes no inherent need to enhance security.

The purpose of this work item is to consider whether there is a need to enhance A/Gb mode security, and if so to develop the necessary security enhancements.

5 Objective

The overall objectives are:

- to complete a threat analysis and security requirements capture for GERAN A/Gb mode. This can be based on the work that was done for UMTS.
- to develop suitable, feasible and cost effective security enhancements for GERAN A/Gb mode if necessary. In particular, the cost effectiveness of upgrading legacy A/Gb mode systems should be considered.

To achieve these objectives the following enhancements will be considered:

- Enhancing the radio interface ciphering mechanism so that it supports key lengths of up to 128 bits.
- Introducing a mechanism for protecting the integrity of signalling data on the radio interface which supports key lengths of up to 128 bits.
- Introducing a security mode negotiation procedure to securely select a ciphering and integrity mode. The procedure should withstand active attacks and allow for the future introduction of new algorithms.

- Introduction of a mechanism for protecting the integrity of user traffic on the radio interface. A similar mechanism to the UMTS mechanism will be considered which protects against insertion and deletion, but not modification of user traffic.
- Specification of suitable ciphering and integrity protection algorithms. Note that A5/3 and GEA3 were designed so that they could be adapted easily to support key lengths of up to 128 bits.
- Specification of handover procedures to and from A/Gb mode, GERAN Iu mode and UTRAN Iu mode.
- Extending the radio interface ciphering for circuit-switched services so that it terminates at least as far back as the BSC rather than the BTS.

GERAN security relies on the existing 3G authentication and key agreement (AKA) mechanism to provide mutual authentication between the MS and the network and to establish session keys for ciphering and integrity of signalling/user data on the radio interface.

6 Service Aspects

None identified yet.

7 MMI-Aspects

Impact on existing security indicators on the UE (e.g. ciphering indicator) will be investigated.

8 Charging Aspects

None identified yet.

9 Security Aspects

The subject of this work item is security.

10 Impacts

Affects:	USIM	ME	AN	CN	Others
Yes		X	X	X	
No					
Don't know	X				

11 Expected Output and Time scale (to be updated at each plenary)

Meeting	Date	Activity
SA3#26	November, 2002	WID approved.
SA3#27	February, 2002	Threat and requirements analysis complete. Start of security architecture definition. Decision taken on whether a new TS is required. Start of algorithm development/selection (if needed).
SA3#28	May, 2002	Security architecture sent to SA plenary for information. Start of stage 3 work.
SA3#29	July, 2002	Security architecture sent to SA plenary for approval.
SA3#30	October, 2002	Corrections to security architecture. Alignment with stage 3 work. Algorithm specifications approved (if needed).

New specifications						
Spec No.	Title	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments
33.xxx	Security architecture	SA3				A decision on whether a new spec is required will be taken at SA3#27

Affected existing specifications				
Spec No.	CR	Subject	Approved at plenary#	Comments

12 Work item rapporteurs

Peter Howard, Vodafone

peter.howard@vodafone.com

13 Work item leadership

TSG SA WG3

14 Supporting Companies

Vodafone, Ericsson, T-Mobile, Polkomtel

15 Classification of the WI (if known)

X	Feature (go to 15a)
	Building Block (go to 15b)
	Work Task (go to 15c)

15a The WI is a Feature: List of building blocks under this feature

- Building blocks may be needed to cover the stage 3 work in the GERAN and CN groups.