Technical Specification Group Services and System Aspects
Meeting #8, Dusseldorf, Germany, 26-28 June 2000

TSGS#8(00)0308

Work Item Description

GERAN security

The GERAN R00 radio access network is a GSM BSS connected via a Iu-ps interface to a packet-switched core network and includes a major redesign of the R99 GSM/GPRS control plane. The GERAN security work item consists of the provision of access link security services such as confidentiality and message integrity between the MS and the GERAN.

1 3GPP Work Area

X	Radio Access
X	Core Network
	Services

2 Linked work items

The work item is linked to other GERAN-related work items.

3 Justification

Compared to GSM/GPRS R99 radio access networks, the upgrade to GERAN R00 includes a major redesign of the radio access network architecture. In order to protect service delivery via GERAN, a security architecture has to be designed that protects against the threats that are envisaged.

4 Objective

The overall objectives are 1) to provide user and signalling data in the GERAN with a level of protection that is as good or better than the level of protection offered in UTRAN and 2) to employ a security architecture that has as much compatibility with the security architecture for UTRAN.

This includes encryption mechanisms applied to both user data and signalling data~~,~~ that extends to a node beyond the base station (if feasible) and uses a symmetric session (ciphering) key of up to 128 bits (if feasible).

This includes integrity mechanisms applied to signalling data and -if possible- also to user data~~,~~ that extends to a node beyond the base station (if feasible) and uses symmetric session (integrity) key of up to 128 bits (if feasible).

This includes security mode negotiation procedures to securely select a ciphering and integrity mode.

This includes the specification of requirements and the selection of suitable ciphering and message authentication algorithms for the above security services.

This includes the specification of handover procedures to and from the legacy GSM BSS and UTRAN.

This work item will study whether after the relocation of the termination of ciphering (and integrity) from the SGSN to the radio access network the LLC layer is still required.

GERAN security relies on the existing UMTS and GSM authentication and key agreement mechanisms to conduct mutual authentication between MS and network and to establish session keys.

5 Service Aspects

The GERAN security features will be generic, i.e., application or service-independent.

6 MMI-Aspects

The GERAN security features will be transparent to the user, with the exception of the mandatory presence of a ciphering indicator in the ME and the ability for users and home networks to configure whether non-encrypted connections are acceptable. These exceptions however will be dealt with in a separate work item that is not radio access network-specific.

7 Charging Aspects

None.

8 Security Aspects

A set of algorithms shall be provided that has withstood peer review.

The security mode negotiation procedure shall withstand active attacks.

The security mode negotiation procedure shall allow for future introduction of new algorithms.

9 Impacts

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

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

Protocol specification

Stage	Date	Action
1	Aug. 00, SA-3#14	GERAN group presents stable GERAN architecture to SA-3
	Sep. 00, SA-3#15	SA-3 specifies the security requirements
	Nov. 00, SA-3#16	SA-3 specifies the security features
2	Jan. 01	SA-3 conducts feasibility study
	Jan. 01	SA-3 specifies GERAN security architecture (Stage 2)
	Mar. 01	SA approves final GERAN security architecture (Stage 2)
3	Feb. 01	SA-3 presents GERAN security architecture to CN, T and GERAN
	Mar. 01	CN, T and GERAN write draft Stage 3 CRs
	Apr. 01	CN, T and GERAN approve final Stage 3 CRs
	Jun. 01	SA-3 reviews final Stage 3 CRs
	Jun. 01	CN, T, RAN approve final Stage 3 CRs

Algorithm specification

Stage	Date	Action
1	Jan. 01	SA-3 specifies the algorithm requirements
	Jan. 01	SA-3 selects a mechanism for algorithm development
	Jan. 01	SA arranges funding
3	Jun. 01	SA-3 approves the algorithms developed
	Oct. 01	3GPP partners publicise algorithm specifications

New specifications						
Spec No.	Title	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments
	??					

Affected existing specifications				
Spec No.	CR	Subject	Approved at plenary#	Comments
33.102		Security architecture	~~January~~March, 2001	
33.103		Security integration guidelines	~~January~~March, 2001	
33.105		Cryptographic algorithm requirements	January, 2001	

11 Work item rapporteurs

~~N.N.~~Bart Vinck, Siemens AG, Tel: +49-89-722 25644, e-mail: bart.vinck@icn.siemens.de

12 Work item leadership

SA 3

13 Supporting Companies

Ericsson, Siemens, T-Mobil

14 Classification of the WI (if known)

	Feature (go to 14a)
X	Building Block (go to 14b)
	Work Task (go to 14c)

14a The WI is a Feature: List of building blocks under this feature

(list of Work Items identified as building blocks)

14b The WI is a Building Block: parent Feature

The work item is child of the feature GERAN.

14c The WI is a Work Task: parent Building Block

(one Work Item identified as a building block)