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

TSGS#8(00)0307

Work Item Description

Evolution of GSM PS algorithms

1 3GPP Work Area

X	Radio Access
X	Core Network
X	Services

2 Linked work items

Visibility and configurability
The user/USIM may need to be able to be request that the terminal indicates which algorithm is used. Furthermore, the user/USIM may need to be able to be request that the terminal rejects communications depending on which algorithm is used.

GERAN security
The recent decision to deploy an Iu-ps interface into the R00 GSN BSC will involve moving PS encryption termination into the GSM BSS. New PS encryption mechanisms and algorithms will therefore need to be developed.

3 Justification

Since the first GSM PS algorithm was developed, export restrictions have been relaxed and the stronger GEA2 can now be deployed. This work item will examine how GEA2 could be rolled out into the network infrastructure and the mobile stations. It will also investigate the development and deployment of new algorithms for the PS domain (see linked work items).

4 Objective

A first objective of this work item is to produce the necessary CRs and to ensure that GEA2 can be deployed.

A second objective will be to investigate the development and deployment of new algorithms for the PS domain (see linked work items).

5 Service Aspects

None identified.

6 MMI-Aspects

There may be an impact on the ciphering indicator (see linked work items).

7 Charging Aspects

None identified.

8 Security Aspects

The main aspect of this work item is security.

9 Impacts

Affects:	USIM	ME	AN	CN	Others
Yes		X	X	X	

No					X
Don't know	X				

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

New milestones have been added (in italics) and some have been removed to supersede the milestones agreed at the joint CN/S3 meeting.

Meeting	**Date**	**Activity**
S3#13	23-26 May 2000	Requirements capture, and identification of all work tasks
	June/July	*Presentation by S2 to S3 of well-defined and understandable system architecture concepts and principles*
CN/S3 joint	*13-14 June 2000*	*Decision to create CRs making GEAx support optional also for R97 to preserve commonality between R97 and R98 and to allow for early roll-out of GEA2 in R97 terminals. Companies to check that no backwards compatibility issues exist.*
CN#8	*21-23 June 2000*	*Final decision on whether GEAx support is optional also for R97.*
SMG#32/SA#8	*June 2000*	*Definition of security architecture: CRs approved at TSG level*
	August 2000	Integration of security architecture: Concept presented to S2 and CN
	September 2000	Integration of security architecture: Complete CRs
	October 2001	Integration of security architecture: CRs approved at TSG level

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				Support for new GSM PS security mechanisms in R00 version of 33.102
33.103				Support for new GSM PS security mechanisms in R00 version of 33.103
33.105				Support for new GSM PS security mechanisms in R'00 version of 33.105

11 Work item raporteurs

12 Work item leadership
TSG SA WG3

13 Supporting Companies
Please mail cbrookson@iee.org if your company is willing to support this work item.

14 Classification of the WI (if known)

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

14a This is a **"Feature".**