Technical Specification Group Services and System Aspects **TSGS#26(04)0864**
Meeting #26, Athens, Greece

3GPP TSG SA WG3 Security ó SA3#36 **S3-041072**
23 ñ 26 November 2004
Shenzhen, China

Title:	**WID for UEA2&UIA2**
Source:	**SA WG3 (agreed at SA WG3 meeting #36)**
Document for:	**Approval**
Agenda Item:	**7.3.3**
Work Item:	**Backup algorithms for UTRAN**

Work Item Description

Title: Development of UEA2 and UIA2

1 3GPP Work Area

X	Radio Access
	Core Network
X	Services

2 Linked work items

None.

3 Justification

SA3 has agreed on the need to develop backup algorithms for UTRAN access confidentiality and integrity protection, the UEA2 and UIA2 to be. There are no current indications that the existing UMTS cipher and integrity protection algorithms (based on KASUMI) are in danger of being broken but cryptanalysis advances all the time. It seems sensible to have a second pair of algorithms developed and deployed in handsets, so that if KASUMI is ever broken, the alternative is ready to use. Of course the new algorithms should be fundamentally different from KASUMI, so that an attack on one algorithm is very unlikely to translate into an attack on the other.

4 Objective

The overall objectives are:

- To develop new algorithms for confidentiality and integrity protection for UTRAN to be in place in mobile terminals should the existing KASUMI-based algorithms be broken in the future.
- To enable operators to quickly and easily re-establish a high level of security by switching their networks to use the new algorithms

The following issues should at least be handled in the WI:

- Confirm GSMA policy and budget allocation to develop new algorithm
- Agree requirement specification with ETSI SAGE for development of new algorithms
- Liaise with GSMA for the commission from ETSI SAGE to develop the new algorithms
- Delivery of algorithm specification, test data and design and evaluation reports

Public evaluation of the algorithm by independent experts is currently not included in the scope. It is SA3's responsibility, based on advice from SAGE, to determine whether public evaluation of the new algorithms is needed.

5 Service Aspects

None identified yet.

6 MMI-Aspects

None

7 Charging Aspects

None

8 Security Aspects

The subject of this work item is security.

9 Impacts

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

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

New specifications						
Spec No.	Title	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments
35.xxx	UEA2 & UIA2 Algorithm Specification	SA3		SA #29 Sept 05	SA #30 Dec 05	
35.xxx	UEA2 & UIA2 Implementorsí test data	SA3		SA #29 Sept 05	SA #30 Dec 05	
35.xxx	UEA2 & UIA2 Algorithm I/O test data	SA3		SA #29 Sept 05	SA #30 Dec 05	
35.xxx	UEA2 & UIA2 Design and evaluation report	SA3		SA #29 Sept 05	SA #30 Dec 05	
35.xxx	UEA2 & UIA2 Final project report	SA3		SA #29 Sept 05	SA #30 Dec 05	

Affected existing specifications				
Spec No.	CR	Subject	Approved at plenary#	Comments
33.102		Support of algorithms		

11 Work item rapporteur(s)

Per Christoffersson, Teliasonera
per.christoffersson@teliasonera.com

12 Work item leadership

TSG SA WG3

13 Supporting Companies

Orange, Vodafone, Nokia, T-Mobile, Gemplus, TeliaSonera

14 Classification of the WI (if known)

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

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

No BBs identified.