3GPP TSG SA WG3 Security — SA3#36 **S3-041014**
23 – 26 November 2004
Shenzhen, China

Work Item Description

Title

Access ~~Network~~ Security ~~Enhancements~~Review

1 3GPP Work Area

X	Radio Access
X	Core Network
	Services

2 Linked work items

None.

3 Justification

SA3 has agreed on short-term solutions to mitigate the worst effects of discovered A5/2 vulnerabilities. SA3 has also agreed that long-term security enhancements are needed to protect GERAN Access Network in the future. A deeper study of GERAN security weaknesses, in particular security dependencies between various uses of the GSM security context, and consideration of potential future attack scenarios is needed, to decide on suitable long-term enhancements of security for GERAN Access Network and other access types relying on GSM security context. Similar considerations for UMTS access security and re-use of UMTS security context also need to be taken account in order to evaluate and re-assess UMTS security features for future attack scenarios, originally not considered.~~.~~

4 Objective

The overall objectives are:

- to complete a threat analysis and security requirements capture for GERAN/UTRAN Access Network and other uses of the GSM and UMTS security contexts.
- to develop suitable, feasible and cost effective long-term security enhancements for GERAN and UTRAN Access Network, and other uses of the GSM and UMTS security contexts
- to develop a cost-effective migration strategy for improving access security in 3GPP systems
- ~~to review if it would be appropriate to introduce any of the proposed GERAN enhancements in UMTS.~~

The following issues should at least be taken into consideration in the study:

- The need and feasibility for network authentication, replay protection and key separation
- Need and feasibility for integrity protection of important signaling messages
- Effects of a near-future break of A5/1, GEA1 and/or other algorithms.
- Risk assessment of implications of “two-time-pads”
- Ensure protection both for the PS and CS domains, in particular that possible insecurity does not spread across domains
- Study effects relating to inter-system handover and security context re-use or re-mapping.
- Consider new threats, e.g. ~~caused~~ repudiation scenarios and effects of using GSM/UMTS security context for other accesses, e.g. WLAN

- Consider security "bottlenecks" arising from different sizes of keys and other security parameters in the various access types, in particular ~~Enhancing~~ enhancing the GERAN radio interface ciphering mechanism so that it supports key lengths of up to 128 bits.
- Study the possibility of using AKA and AKA based applications for enhancing security.

When it comes down to the level of cryptographic algorithms, the aim of the study is NOT to attempt to cryptanalyze any of the GSM/UMTS algorithms, but rather to ask "what if this is broken" type questions.

5 Service Aspects

None identified yet.

6 MMI-Aspects

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

7 Charging Aspects

None identified yet.

8 Security Aspects

The subject of this work item is security.

9 Impacts

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

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
33.xxx	~~Feasibility Study on Access Network Security Enhancements~~Access Security Review	SA3		SA #28	SA #29	

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

11 Work item rapporteur(s)

Bengt Sahlin
Bengt.Sahlin@ericsson.com

12 Work item leadership

TSG SA WG3

13 Supporting Companies

Ericsson, Qualcomm Europe, Vodafone, Telenor

14 Classification of the WI (if known)

	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

(list of Work Items identified as building blocks)

14b The WI is a Building Block: parent Feature

(one Work Item identified as a feature)

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

(one Work Item identified as a building block)

form change history:
v1.11.0: includes those changes from v1.8.0 agreed at SP-25.
v1.10.0: full circle
v1.9.0: a clean sheet
v1.8.0: includes comments from SA#24
v1.7.0: includes comments from RAN, CN and T #24; also includes “early implementation” data
v1.6.0: includes comments made during review period prior to TSGs#24
v1.5.0: includes comments made at TSGs#23 (Phoenix)
v1.4.0: offered to SA#23 for approval
v1.3.0: offered to CN#23, RAN#23 and T#23 for comments
DRAFT4 v1.3.0: 2004-03-09: Incorporation of comments from Leaders list
DRAFT3 v1.3.0: 2004-02-19: Incorporation of comments from MCC members
DRAFT2 v1.3.0: 2004-01-29: Complete redraft:
v1.2.0: 2002-07-04: "USIM" box changed to "UICC apps"
2003-05-28: spelling of “rapporteur” corrected
2002-07-04: "USIM" box changed to "UICC apps"