3GPP TSG SA WG3 Security — S3#15 **S3-000511**

12-14 September, 2000

Washington D.C., USA

Source:	**Telenor**
Title:	**Proposed update of WI Network Domain Security**
Document for:	**Decision**
Agenda Item:	**-**

Introduction

The following is a proposed update of the WI on network domain security. As announced on the S3 mailing list there are some minor changes:

- Changing the name of the WI from **Core Network Security** to **Network Domain Security**. The motivation is mainly to make it clear that the Iu-interface properly belongs to this WI, and it was though that the new name better reflects this.

- It has been further clarified that this WI covers the Iu-interface. The motivation here is to include all interfaces where CK/IK is transported. Strictly speaking, this also means that the Iur-interface must be protected (as far as I understand it, RNC's exchange keys over Iur during handover).

- The rapporteur name has been changed according to the decision made at SA3#15

Since the changes are minimal I have not included revision marking to the main text. The change in the time plan is marked.

Decisions to be made

CAP security?

S3 is asked to make a decision on whether or not we shall try to secure CAP. This far nobody has actually produced any input on either requirements or feasibility of securing CAP. According to our time plan we should by now be ready to specify CAP security. Given this, S3 is asked to reconsider:

a) Should we still include CAP, but with revised time plan?

b) Should we remove CAP from the time plan?

Security for the A-interface?

S3 should also consider whether it is a good idea to try to retrofit security for the A interface. The A-interface is based on SS7 and a solution should probably be found on the application level (BSSAP). If the main purpose is to protect the key **Kc**, it will be enough to provide confidentiality for the BSSMAP information element ENCRYPTION INFORMATION (which contains **Kc**), but if generic security is required a lot of work is required here.

a) Shall we exclude the A-interface from this WI?

b) Shall we limit our scope to only protect the key transfer?

c) Shall we try to secure the A-interface (BSSAP) on the same level as we do for MAP?

/Geir M. Køien

Work Item Description

Title

Network Domain Security
(formerly called the Core Network Security)

1 3GPP Work Area

X	Radio Access
X	Core Network
	Services

2 Linked work items

- Related work is in RAN3, N2 and N4 to specify the solutions developed by S3.

3 Justification

An identified security weakness in 2G systems is the absence of security in SS7 networks. This was formerly perceived not to be a problem, since this network was the province of a small number of large institutions. This is no longer the case, and so there is now a need for security precautions.

This work item describes ongoing work in S3, which had been originally tasked by SA to S3 under the name of “MAP Security”, an early version of which had originally been included in R’99.

4 Objective

Various protocols and interfaces are used for signaling in and between core networks. These include among the applications MAP, CAP, and GTP, among the interfaces Iu, A, and Iur, and possibly other applications or interfaces that are new to R’00 or have yet to be identified. The security characteristics that have been identified as being in need of protection are confidentiality, integrity, and authentication. These will be ensured by standard procedures, based on cryptographic techniques.

This work might also be extended to protection of the user plane.

Within this WI MAP Application Security has been separated out into its own work item as a sort-of minimal solution, for completion for R’00; MAP-over-IP is foreseen as belonging to this WI proper and not to the minimal solution. In addition, the protection of GTP has a high time priority; completion of this aspects of the feature is expected well in advance of the others.

5 Service Aspects

None identified.

6 MMI-Aspects

None identified.

7 Charging Aspects

None identified.

8 Security Aspects

The work item is a security item.

9 Impacts

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

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

Meeting	Date	Activity
CN/S3 joint meeting	June 13-14, 2000	Presentation by S2 of R'00 architecture
CN	July-August, 2000	Specification of the protocol stacks of the core network interfaces
S3	June-July, 2000	Requirements capture GTP signalling security Feasibility study of GTP signalling security, including definition of work tasks and completion of plan
S3#14	August 1-4, 2000	Requirements capture (CAP, MAP-over-IP, etc.) Feature specification of GTP signalling security
S3#15	September 12-15, 2000	Specification of other security features (CAP, MAP-over-IP, etc.) Approval of GTP CRs
SA#9	September 25-28, 2000	Approval of GTP CRs
N4#5	November 13-17, 2000	N4 approval of GTP CRs
S3#16	November 27-30, 2000	Feasibility study, including definition of work tasks and completion of plan. Requirements capture for security over A, Iu and Iur interfaces.
CN#10	December 6-8, 2000	Approval of GTP CRs
S3#17	January, 2001	Definition of security architecture, first draft
S3#18	February, 2001	Approval of CRs to the drafts Integration of security architecture (presentation to other WGs)

S3#19	March, 2001	S3 approval of final versions
SA#12, CN#12	June, 2001	Approval of final versions

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				Re-inclusion and extension of core network signalling security in 33.102 (R'00 for MAP and GTP, R'01 for the rest)
33.103				Re-inclusion and extension of core network signalling security in 33.102 (R'00 for MAP and GTP, R'01 for the rest)
33.105				Inclusion of core network signalling security algorithm requirements in 33.102 (R'00 for MAP and GTP, R'01 for the rest)

11 Work item raporteurs

Geir M. Køien, Telenor
Geir-myrdahl.koien@telenor.com
Tel +47 9075 2914
Fax +47 3704 5284

12 Work item leadership

TSG SA WG3

13 Supporting Companies

T-Mobil, Vodafone, Ericsson, Telenor, Nokia, Siemens, Motorola

14 Classification of the WI (if known)

X	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

Network Domain Security: protection of MAP Application Layer
Network Domain Security: key exchange and distribution
Other possibilities:
GTP signalling security
CAMEL signalling security
Building blocks from N2, N4, S2, S5

14b The WI is a Building Block: parent feature „provision of IP based multimedia services“