

Work Item Description

Title

Key management for core network security

1 3GPP Work Area

	Radio Access
X	Core Network
	Services

2 Linked work items

MAP application layer security

The MAP application layer security work item involves the protection of MAP dialogues between core network elements by integrating protection mechanisms into the MAP application. This allows for MAP-over-SS7 links to be protected with no impact on the SS7 stack.

Core network security

The core network security work item involves the extension of the minimal solution to cover other applications and interfaces including GTP signalling. The full solutions will also look at mechanisms to protect new core network interfaces and applications which are introduced in the R00 system architecture.

3 Justification

Two other work items on core network security are tasked with defining mechanisms to protect traffic on transmission links within the core network. These mechanisms will require the necessary keys to be established at each involved network element. Because of the number of keys involved and the rate at which they must be changed, it is desirable for an automated key management mechanism to be used. In order to support inter-operation between operators and multi-vendor core networks, it is also desirable for such a solution to be standardised.

4 Objective

The main objective of this work item is to specify key management standards for core network security including MAP application layer security. The mechanisms specified must allow for scaleable, flexible and cost-effective architecture(s) to be built to support key management towards core network elements. This work item will also study the management of security policies between network elements.

5 Service Aspects

None identified.

6 MMI-Aspects

None identified.

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	
No	X	X	X		X
Don't know					

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

Dates for the IP/IKE-based solution to be added at S3#14.

Meeting	Date	Activity
CN/S3 joint meeting	June 13-14, 2000	Feedback from CN about the practicability of an IP/IKE-based key management solution versus the previously specified ISO-based solution for which N4 have developed CRs to implement the protocols using MAP.
	June/July, 2000	Contributions solicited to determine if MAP-based key management is to be specified.
S3#14	August 1-4, 2000	Decide whether a MAP-based key management solution will be specified. Decide on dates for and IP/IKE-based solution.
CN#9	September, 2000	Completion of MAP-based key management CRs by CN (if S3 decided to work on this solution).

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 of core network signalling security key management architecture in a R00 version of 33.102	
33.103					Re-inclusion of core network signalling security key management architecture in a R00 version of 33.103	
33.105					Inclusion of core network signalling security key management architecture algorithm requirements in a R'00 version of 33.105	

11 Work item rapporteurs

Peter Howard, Vodafone
Peter.Howard@vf.vodafone.co.uk
 Tel +44 1635 676206
 Fax +44 1635 231721

12 Work item leadership

TSG SA WG3

13 Supporting Companies

Siemens
 Motorola
 Telenor
Vodafone

14 Classification of the WI (if known)

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

14b The WI is a Building Block: parent Features/Building Blocks “core network security: full solution” and “core network solution: minimal solution”.