Technical Specification Group Services and System Aspects Meeting #11, Palm Springs, CA, USA, 19-22 March 2001

TSGS#11(01)0153

3GPP TSG SA WG3 Security — S3#17 **<revision of S3-010123>**

27 February - 02 March, 2001

Gothenburg, Sweden

Work Item Description

Network-based end-to-end security

1 3GPP Work Area

X	Radio Access
X	Core Network
X	Services

2 Linked work items

There are five related work items in S3:
- User plane protection in access network
- Access security for IP-based services
- Core network security: full solution
- Lawful interception in the REL-5 architecture
- Visibility and configurability

3 Justification

The REL-5 system architecture may create new requirements and/or opportunities for extending user plane traffic security further back into the core network. In addition it may allow for security mechanisms to be applied on an end-to-end basis, providing that the necessary lawful interception requirements are addressed when encryption is applied. ~~This work will take advantage of concepts and hooks for network-wide encryption which have been considered in R99.~~

4 Objective

The overall objective of this WI is to specify a network-based security architecture which provides security features to users on an end-to-end basis. ~~The architecture is expected to be based on an evolution / re-use of the existing R99 security architecture.~~ The work will study the specification of end-to-end security for CS domain, PS domain and IM core network subsystem.

The main security feature to be provided is expected to be encryption. However, the specification of other security features (e.g. authentication and integrity protection) will also be investigated.

The work may involve defining an appropriate key management architecture to support the end-to-end security mechanisms and the integration of thiese into the system architecture. Where possible this would be based on an evolution / re-use of the existing R99 authentication and key agreement mechanism. Some key management concepts for end-to-end security were presented in an old version of the R99 security architecture (33.102 v3.4.0).

The work may involve the specification of the end-to-end security mechanisms and the integration of these mechanisms into the system architecture. This work would involve the specification of an end-to-end security mode control mechanism which will handle algorithm selection, mode selection and user control. It would also involve the specification of any necessary end-to-end synchronisation mechanisms.

5 Service Aspects

Service requirements for end-to-end security need to be identified and addressed in conjunction with S1.

6 MMI-Aspects

Visibility and configurability of end-to-end security will be important. For example, the existing ciphering indicator may need to be enhanced to indicate whether or not the call is encrypted on an end-to-end basis.

7 Charging Aspects

End-to-end security may be considered to be a value-added service, especially if it is not, or cannot, be provided as a default.

8 Security Aspects

The main aspect of this work item is security.

9 Impacts

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

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

Meeting	Date	Activity
S3~#17	February 2001	Agreement of work item ~~and CR to reintroduce text removed from R99~~
	April 2001	Definition of Work Tasks and completion of the plan for this Feature
S3#18	May 2001	Feasibility study and definition of security architecture~~: new CRs approved~~
S3#19	July 2001	Concept presented to CN, RAN, T and GERAN
S3#20	October 2001	Integration of security architecture~~: Complete CRs~~
S3#21 and SA#14	December 2001	~~Integration of security architecture: Crs~~Specifications approved at TSG level

This table will be finalised when the plan for this feature is complete (see milestones above)

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				
33.103				
33.105				

11 Work item raporteurs

~~Peter Howard~~
~~Communications Security and Advanced Development~~
~~Vodafone Ltd~~
~~The Courtyard~~
~~2-4 London Road~~
~~Newbury~~
~~RG14 1JX~~
~~Phone +44 1635 676206~~
~~Fax +44 1635 231721~~
~~peter.howard@vf.vodafone.co.uk~~
Colin Blanchard
colin.blanchard@bt.com

12 Work item leadership

TSG SA WG3

13 Supporting Companies

~~Draft list: Vodafone,~~ BT, Nortel, Lucent, Gemplus

14 Classification of the WI (if known)

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