3GPP TSG SA WG3 Security — S3#19 **S3-010346**

3 - 6 July, 2001

Newbury, GB

Source: **Lucent**

Title: **Work Item Description for "End-to-End VoIP Privacy"**

Document for: **Discussion & Action**

Agenda Item:

Abstract:

This contribution proposes an amendment to the Network Wide End to End Encryption of user traffic to 3G TS 33.102 'Security Architecture' WI. Change bars indicate the differences to the WI description as presented in S3-010090 in Gothenburg.

The work item is amended to cover the necessary functionality and services required to provide End – to – End voice privacy over an IP transport protocol (VoIP).

The work will involve defining an appropriate, possibly independent, key management architecture to support the end-to-end encryption mechanism and the integration of this mechanism into the overall architecture.

To achieve best performance, this work item proposed that the encryption and synchronization should be codec-based, i.e. adjacent to the codec. It further proposes that the key management may also be codec-based, therefore minimizing system involvement and thus speed deployment.

Work Item Description

~~Network-based end~~End-to-end security ~~for~~ for Voice in the IM subsystem (VoIP)

1 3GPP Work Area

~~X~~	~~Radio Access~~
X	Core Network
X	Services
X	Codec

2 Linked work items

There ~~are five~~is a related work item~~s~~ in S3:
~~User plane protection in access network~~
~~Access security for IP-based services~~

~~Core network security: full solution~~
~~Lawful interception in the R00 architecture~~
Visibility and configurability

3 Justification

~~The R00 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.~~ Migration of telephone switching networks to IP networks opens more opportunities for security compromise of a link-encrypted connection. Content may be carried by IP backbone providers, whose security mechanisms are out of the domain of the service provider. In addition, the mobile owner may confuse proprietary IP networks with the public Internet. Therefore the end-to-end encryption capability is proposed to mitigate the above problems while reducing network complexity and enhancing network performance.

AMR voice traffic has unique attributes: It is real-time, error-tolerant, and does not allow bandwidth expansion over the air interface. These attributes require an end-to-end encryption treatment that differs from what might be applied to other types of content, such as generic IP data.

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.~~ an end-to-end VoIP encryption architecture. It should be noted that encrypting the voice traffic carried over the CS domain is not part of this WI, although this architecture may be applicable to CS as well as to PS domains.

~~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 will ~~may~~ involve defining an appropriate, possibly independent, key management architecture to support the end-to-end encryption mechanism ~~security mechanisms~~ and the integration of this ~~these~~ into the overall ~~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 also 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 include ~~involve~~ the specification of any necessary end-to-end synchronisation mechanisms.

To achieve the best performance, the encryption and synchronization should be codec-based, i.e. adjacent to the codec. To minimise system involvement and thus speed deployment, that the key management may also be codec-based.

5 Service Aspects

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

6 MMI-Aspects

Visibility and configurability of end-to-end VoIP privacy ~~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 VoIP privacy ~~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 VoIP privacy.~~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~~19	~~February~~ July 2001	Agreement of work item ~~and CR to reintroduce text removed from R99~~
	~~April~~ July 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 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~~

12 Work item leadership

TSG SA WG3

13 Supporting Companies

Draft list: ATT-WS, Motorola, Gemplus, and ~~Vodafone, BT, Nortel,~~ Lucent

14 Classification of the WI (if known)

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