

2-4 August, 2000

Oslo, Norway

Source: SA WG3

Title: Draft LS on UE triggered authentication and key agreement during connections

Document for: Approval

Agenda Item: 12

From: TSG SA WG3¹

To: TSG CN WG1

Copy: TSG RAN WG2, TSG T WG3

Title: LS on UE triggered authentication and key agreement during connections

S3 thanks N1 for their LS (N1-000797=S3-000402) which responds to an LS from S3 concerning UE triggered authentication and key agreement during connections (S3-000213).

S3 have created a WI to develop the stage 2 specifications for this security feature (see draft WI description attached). It is planned to present this WI to SA#9 for approval and to integrate the WI into the overall R00 project plan. It is expected that the stage 3 specifications will be developed by N1 and that a corresponding WI description will be produced by N1. Note however that there may also be an impact on R2 and/or T3 specifications but this cannot be determined until the stage 2 specifications have been developed.

¹ Contact: Peter Howard,

Email. peter.howard@vf.vodafone.co.uk

Tel. +441635 676206

2-4 August, 2000

Oslo, Norway

Source: SA WG3**Title:** WI description for UE triggered authentication during connections**Document for:** Approval**Agenda Item:** 11**Work Item Description****Title****UE triggered authentication during connections****1 3GPP Work Area**

X	Radio Access
X	Core Network
X	Services

2 Linked work items

None identified

3 Justification

The R99 security architecture specifies a mechanism to allow the UE to force an authentication at the start of an RRC connection if the value of the hyperframe number at the end of the previous RRC connection exceeds an operator determined threshold value contained on the USIM. The mechanism is used to help control the lifetime of the cipher and integrity keys, CK and IK, by reducing the reliance on the serving network to implement an appropriate authentication policy.

It is intended to enhance this mechanism in R00 so that the authentication and key agreement procedure can be triggered by the UE during a connection if the threshold hyperframe number is reached. This may be useful if long connections are expected (e.g. in the PS domain).

4 Objective

The objectives of this work item are:

- to produce the necessary stage 2 specifications
- to ensure that the stage 3 specifications are developed by the relevant groups

In order to implement this feature, it is required that the UE is able to indicate to the core network during a connection that the authentication procedure should be run.

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
Don't know	X	X	X		

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

Meeting	Date	Activity
S3#15	September 2000	Stage 2 specifications complete.
S3#16	November 2000	

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						

11 Work item raporteurs

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

BT, Nokia, Motorola, Vodafone

14 Classification of the WI (if known)

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