b3GPP TSG SA WG3 Security — S3#22 **S3-020315**

14 - 17 May 2002

Victoria, Canada

Title: Reply LS on key expansion for HMAC-SHA-1-96

Response to:

Source: 3GPP SA3

To: ETSI SAGE

Cc:

Contact Person:

Name:	**Peter Howard**
Tel. Number:	+ 44 1635 676206
E-mail Address:	Peter.Howard@vodafone.com

Attachments: None

---

1. Overall Description:

SA3 have proposed that HMAC-MD5-96 [RFC2403] and HMAC-SHA-1-96 [RFC2404] shall be used for integrity protecting SIP messages between the mobile and the network as part of the IP multimedia subsystem (IMS) security architecture which is standardised in 3GPP TS 33.203 (Release 5).

IMS security uses the same authentication and key agreement protocol as used for UMTS access security. This protocol generates a 128 bit integrity key (IK). As HMAC-SHA-1-96 requires a 160 bit key, SA3 have proposed a simple expansion function which appends the first 32 bits of the IK to itself to obtain the 160 bit key. An alternative solution which appends 32 “0” bits to IK was also discussed.
Note that it does not seem possible to generate a key with an effective key length of 160 bit without substantial changes to the IMS authentication procedures.

SAGE are asked to comment the suitability of the proposed expansion function and the alternative proposal.

2. Actions:

To SAGE group.

ACTION: **SA3 asks SAGE to comment on the suitability of the proposed expansion function and the alternative proposal for HMAC-SHA-1-96.**

3. Date of Next TSG-SA3 Meetings:

SA3#24	9th – 12th July 2002	Helsinki, Finland
SA3#25	8th – 11th Oct 2002	Munich, Germany