3GPP TSG SA WG3 Security — S3#33 **S3-040268**
10 - 14 May 2004
Beijing, China

ETSI SAGE **SAGE (04) 01**

29 April 2004

Title: SAGE work on key derivation for the Generic Bootstrapping Architecture
Response to: LS S3-040162 "LS on key derivation for the Generic Bootstrapping Architecture"
Source: ETSI SAGE
To: 3GPP SA3
Cc:

Contact Person:
Name: **Steve Babbage**
Tel. Number: + 44 1635 676209
E-mail Address: steve.babbage@vodafone.com

Attachments: None

Introduction

The liaison from SA3 asked:

> *3GPP SA3 kindly asks ETSI SAGE to assist in completing the specification of TS 33.220 by providing a specification for a key derivation function satisfying the requirements outlined in this LS. If SAGE agrees to take the work on 3GPP SA3 would also appreciate if SAGE could indicate a time-frame for the completion of the work by sending a reply to SA3's meeting in May. The work should be completed within the deadline for 3GPP Release 6. Unfortunately, the precise deadline is not known yet, but it is expected that the SA plenary will decide it in March. It will then be communicated to SAGE. Any further observations by ETSI SAGE would, of course, also be welcome. If more information is required SAGE is kindly asked to contact SA3.*

Response

Yes, we can propose a function. We propose to do this by Friday 11th June, provided that our questions below are answered by Friday 21st May (an informal answer is fine, e.g. in person from Peter Howard to Steve Babbage). We hope that this will allow SA3 enough time to incorporate our proposal in to the standards for approval at their July meeting.

Initial thoughts

We are expecting the function to have the following form:

INPUTS

Ks	256 bits
IMSI	15 decimal digits — we propose to encode this as 15 octets, each octet being an ASCII representation of the appropriate character between '0' (30 hex) and '9' (39 hex)
NAF_Id	We assume that this is an ASCII-coded text string of arbitrary length
RAND	128 bits

OUTPUT

Ks_NAF	256 bits

Given the required output size, our current thoughts are that the natural algorithm choice is HMAC-SHA-256, using Ks as key and concatenating the other parameters to form the "text" input. This concatenation must be done in a unique and unambiguous way. We propose to let

"text" = FC || RAND || IMSI || NAF_Id

where:

- FC is a single octet having a fixed value, say 00 hex — its purpose is to allow this KDF to be considered as one of a family of up to 256 algorithms, to allow for future variants for different purposes;
- RAND and IMSI have fixed length (16 and 15 octets respectively);
- thus the "text" length is 32 octets greater than the length of NAF_Id.

Questions

Are we right to interpret NAF_Id as an arbitrary length ASCII-coded text string?

Is it OK to fix the IMSI length as 15 digits, or might it be necessary to support longer IMSIs in future?

Will a representation of IMSI as ASCII-coded characters be convenient, or would some other format be better (e.g. binary coded decimal)?

Are you happy with the use of HMAC-SHA-256? (We could use HMAC-SHA1 if only 160 bits of output were required, and HMAC-SHA1 may well be implemented by manufacturers already. SA3 may wish to consider how important the requirement is to support outputs greater than 160 bits.)

Do you have any other comments on our tentative proposal?