3GPP TSG SA WG3 Security — S3#28 **S3-030219**
6 - 9 May 2003
Berlin, Germany

ETSI SAGE **SAGE (03) 01**

30 April 2003

Title: Initial response on key derivation for IMS-based application services
Response to: LS S3-030147 "LS on key derivation for IMS-based application services"
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

SA3 have asked SAGE about the feasibility of deriving several symmetric keys DKi, to secure links between the UE and various end-points, from the cipher key CK.

Comments

SAGE does believe that key derivation of the form suggested is possible, providing an acceptable level of security.

Our particular assumptions/comments/suggestions are as follows:

- From SA3's LS it was unclear whether the key derivation should be on the terminal or the USIM. From further discussion we understand that it should be on the terminal.
- In the IMS context we expect the following algorithms to be present on the terminal already: HMAC-SHA1, HMAC-MD5, and possibly Kasumi. Of these, HMAC-SHA1 is probably the most useful building block.
- It is certainly not sufficient to use only CK and the application identity ASi as inputs to the key derivation, because of the danger of a collision between two instances of CK (between users or for the same user).
- Taking RAND, user-specific name (e.g. IMS Private ID) or both as additional inputs seems sufficient at a first analysis — there is no obvious reason why newly generated nonces are required. We would like to spend a bit more time thinking about this, though.
- It seems sufficient for the 128-bit CK to be the only secret input to the key derivation. Any attempt to introduce additional secret input would be fairly artificial anyway, since in the end this all hangs on the 128-bit long-term user secret key.

SAGE is very willing to help define a key derivation mechanism, on the following understanding:

- The problem that SAGE is asked to solve should be as well defined as a cryptographic problem, and as abstracted from the context, as possible. The communication to SAGE contained rather a lot of contextual information. We don't understand the details of these systems as well as you do!
- SAGE is expected to provide a fairly brief definition of any key derivation algorithm — we are not expected to provide a full standalone specification with test vectors, C code etc.
- SA3 will specify an input parameter ASi that is well-defined and uniquely identifies each application server — SAGE is not expected to do this.