3GPP TSG-SA WG3 Meeting #33 **S3-040408**
Beijing, China, 10th – 14th May 2004.

Title:	[DRAFT] Response to LS (S3-040268) on key derivation for the Generic Bootstrapping Architecture
Release:	Rel-6
Work Item:	GBA
Source:	SA3
To:	ETSI SAGE
Cc:	

Contact Person:
Name: **Adrian Escott**
Tel. Number: +44 7782 325254
E-mail Address: adrian.escott@three.co.uk

Attachments: Explanation slides

1. Overall Description:

SA3 thank ETSI SAGE for their liaison concerning key derivation for the Generic Bootstrapping Architecture

ETSI SAGE asked SA3 several questions in their LS. SA3 provide the answers below:

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

SAGE can assume NAF_Id is an arbitrary-length bit-stream and the coding of it will be specified by SA WG3.

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

No, as IMPI is the currently preferred identity by SA3. The identity will be an arbitrary-length bit-stream and the coding will be defined by SA WG3.

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

Obsolete due to second answer.

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.)

SA3 require an output of 256 bits.

Do you have any other comments on our tentative proposal?

SA3 have expanded the scope of GBA to include enhanced UICCs (see attached slides for more information). These UICCs can be instructed to perform a special run of GBA, where one key, called Ks_int, remains on the UICC and a second key, called Ks_ext, is output from the UICC. Both Ks_int and Ks_ext are used to derive NAF specific keys Ks_int_NAF and Ks_ext_NAF respectively. Ks_int_NAF does not leave the UICC.

Deriving Ks_ext_NAF from KS_ext is exactly identical to deriving Ks_NAF from Ks. Similarly deriving Ks_int_NAF from Ks_int is identical in terms of available inputs to deriving Ks_NAF from Ks except the calculation takes place on the UICC. The functions used to derive Ks_int_NAF and Ks_ext_NAF do not have to be identical.

In additional there is a need to derive Ks_ext from Ks_int = CK || IK in the UICC. This derivation will happen in the UICC and the Boot Strapping Function (BSF) and hence the possible inputs to the derivation function are limited to data known at these two places, e.g. AVs and subscriber identity.

A further option under discussion is to have all the key derivations in the UICC (this is shown in the last slide).

SA3 hope that this extended scope is acceptable to ETSI SAGE and ask ETSI SAGE to take into the above information when designing the KDF(s).

2. Actions:

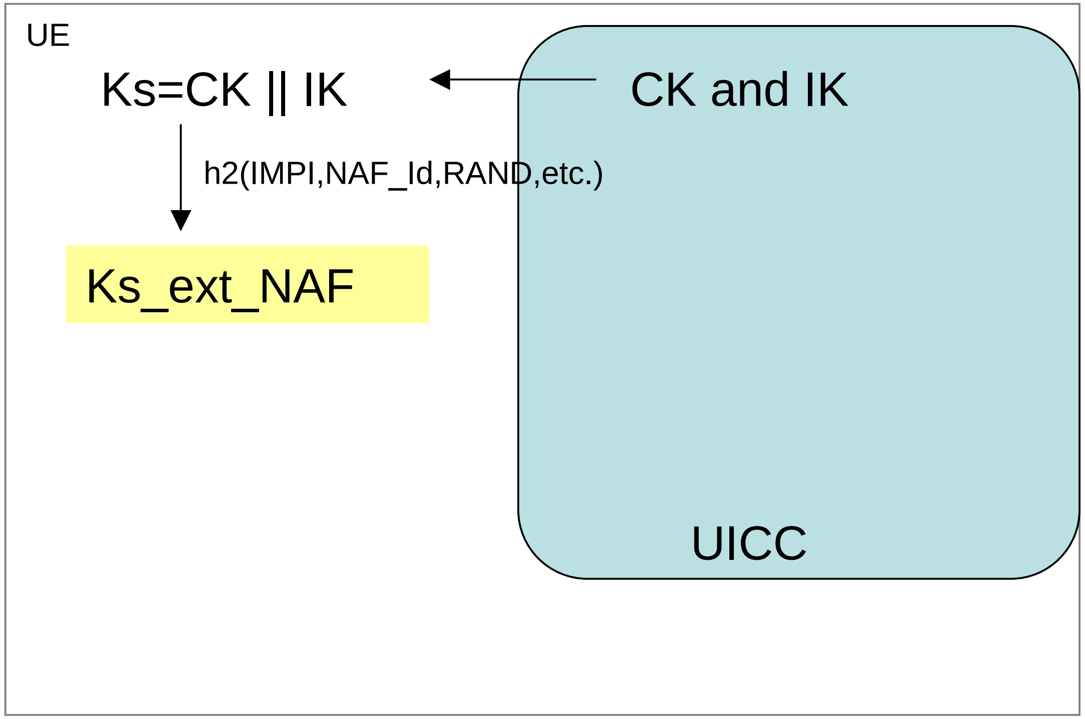
To ETSI SAGE group.

ACTION: SA3 asks ETSI SAGE to take into the above information when designing the KDF(s).

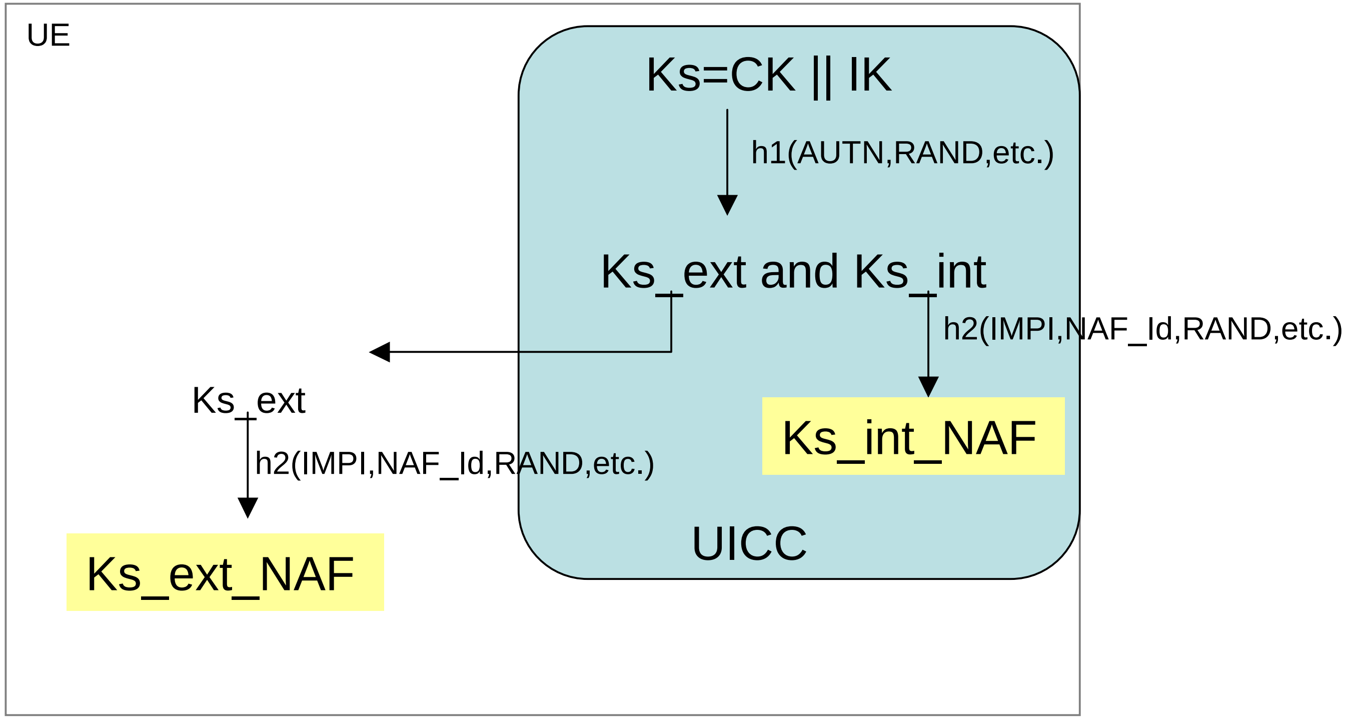
3. Date of Next TSG-SA WG3 Meetings:

TSG-SA WG3 Meeting #34	6th – 9th July 2004	Acapulco, Mexico
TSG-SA WG3 Meeting #35	5th – 8th October 2004	Malta

KDF with a GBA-unaware UICC

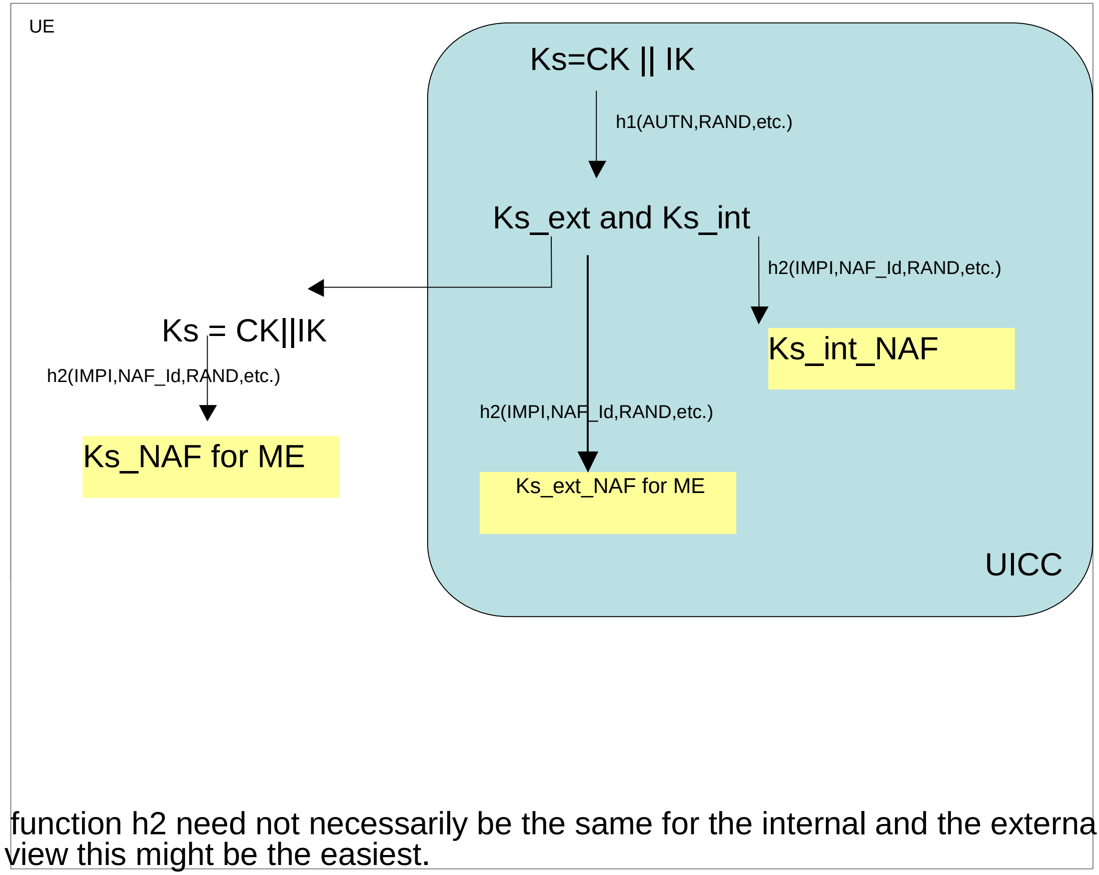


KDF with a GBA-aware UICC for special run



- Note: The KDF function h2 need not necessarily be the same for the internal and the external key, but from a design point of view this might be the easiest.

Further option with Ks_int and Ks_ext in UICC



- Note: The KDF function h2 need not necessarily be the same for the internal and the external key, but from a design point of view this might be the easiest.
- Note: Ks is only given out of UICC if the UICC is not asked for special run. In this case Ks_int and Ks_ext are not calculated .