3GPP TSG SA WG3 Security — SA3#33 **S3-040225**
10-14 May 2004
Beijing, China

Source:	**Siemens**
Title:	**MBMS key management scenarios and GBA**
Document for:	**Information**
Agenda Item:	**GBA and MBMS**

Cover sheet for included presentation

The attached presentation contains an overview of MBMS scenarios and the use of GBA. The presentation can be used in conjunction with documents S3-040218 (GBA_U concept), S3-040219 (pCR on TS 33.246: using GBA for MBMS) and S3-040217/216 CRs on TS 33.220.

MBMS scenarios and the use of GBA

Siemens

9 April 2004

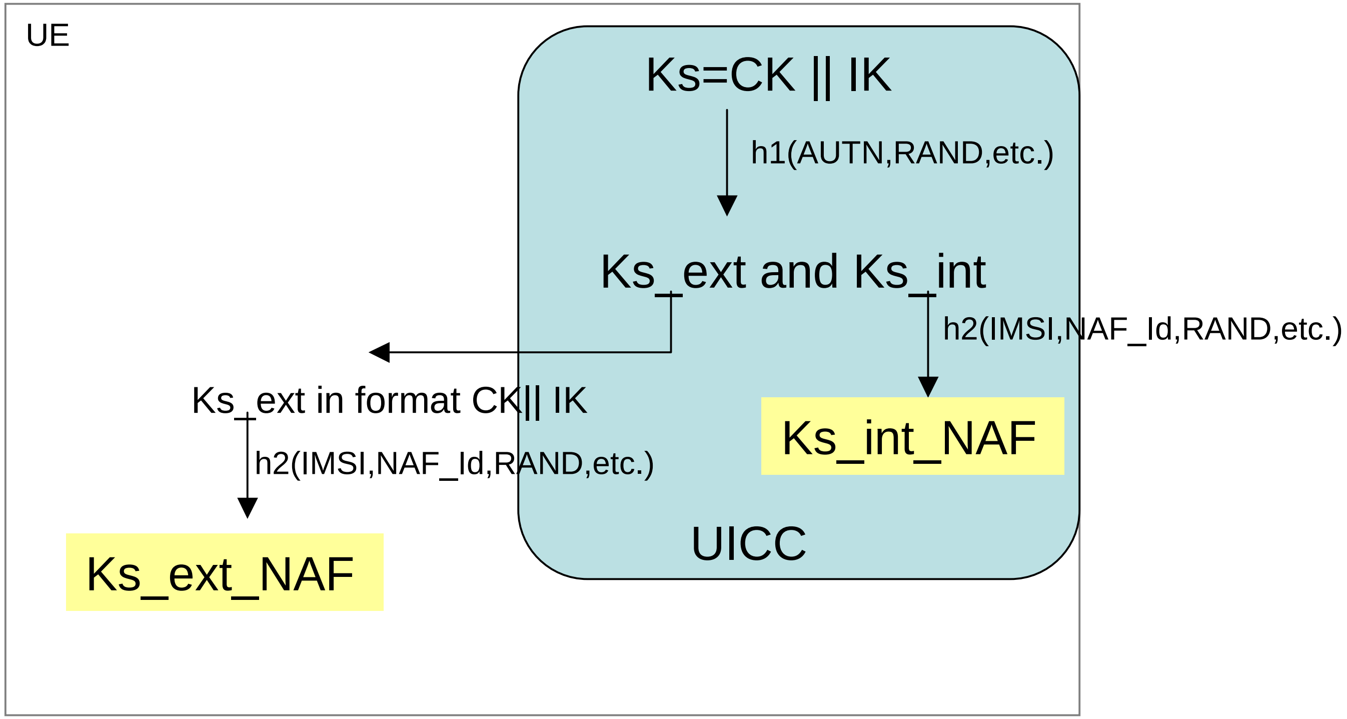
Content

- GBA
  - – Definitions
  - – Key derivation functions
- Feature relationships MBMS and GBA
- Analysis of scenarios (MBMS view)
  - – ME based Key Management & UICC based key Management
  - – A view on the GBA details

Definitions

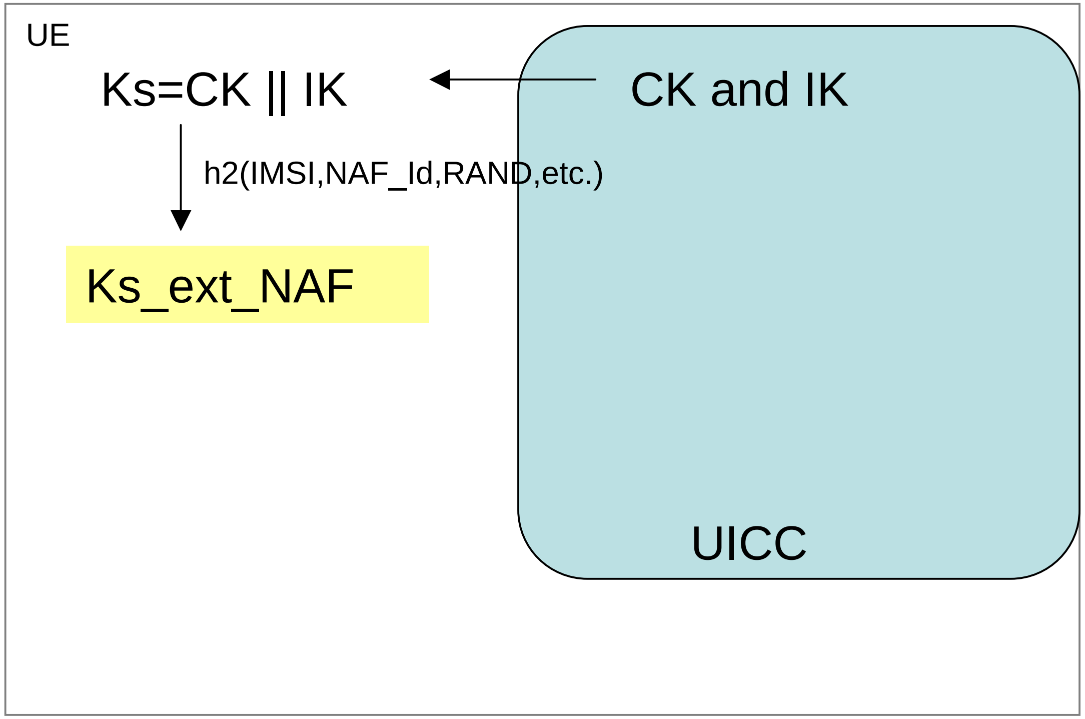
- **A GBA aware UICC:** A UICC capable of deriving **both** Ks_int and Ks_ext whereby Ks_ext is given to the ME and whereby the Ks_int (and subsequent derived Ks_int_NAF) are kept secret within the UICC.
- **A GBA unaware UICC**: A UICC not containing the above described functions (e.g. All currently available UICC's)

Proposed KDF with a GBA-aware 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.

Existing KDF with a GBA-unaware UICC



Feature dependencies: MBMS and GBA

- There are 2 possibilities for the Rel6 ME
  1) A Rel-6 ME supporting MBMS **SHALL** support both ME based key management and UICC based key management
  2) A Rel-6 ME supporting MBMS **SHALL** either support ME based key management or support UICC based key management.
  - Option 1 limits the possible interworking cases (scenarios) and complexity.
- To run ME based key management:
  - Required ME features: GBA_ME needs to be supported: includes GBA_ME network procedures (Ub), KDF on the ME. (subset of GBA_U)
- To run UICC based key management:
  - Required ME features:
    - GBA_U needs to be supported : Includes GBA_U network procedures (Ub) , Interface procedures towards the UICC for generating UICC internal key Ks_int(_NAF) (KDF on the UICC) and handling Ks_ext (KDF on the ME).
    - Needs to support MBMS UICC key management interface procedures.
  - Required UICC features:
    - UICC shall contain an MBMS key management application and shall be GBA aware.

Scenarios resulting in ME based Key Management (network and UE view)

- Basic scenarios (slide 6 option 1)
  - – Scn-1a: UICC has no MBMS application
  - – Scn-1b: UICC has an MBMS application but HSS and BSF have not been upgraded to use GBA_U.
  - – Scn-1c: UICC has an MBMS application, HSS and BSF support GBA_U, but not the BM-SC.
- Additional scenarios (if slide 6 option 2 is allowed)
  - – Scn-1d: UICC has an MBMS application, but the Rel-6 ME does not support UICC based key management.

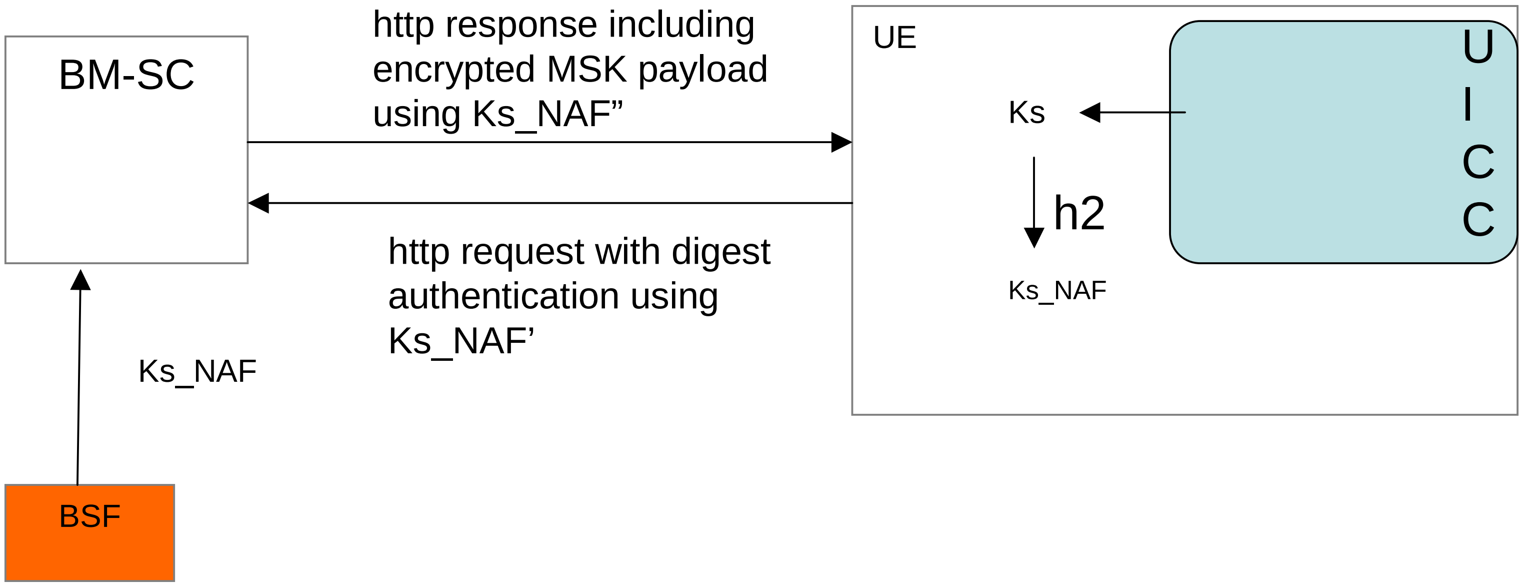
Scenarios resulting in UICC based Key Management (network and UE view)

- Basic scenario
  - Scn-2: Both the network and UE have to support all required functions to allow UICC based key management (cf slide 6)

GBA-view

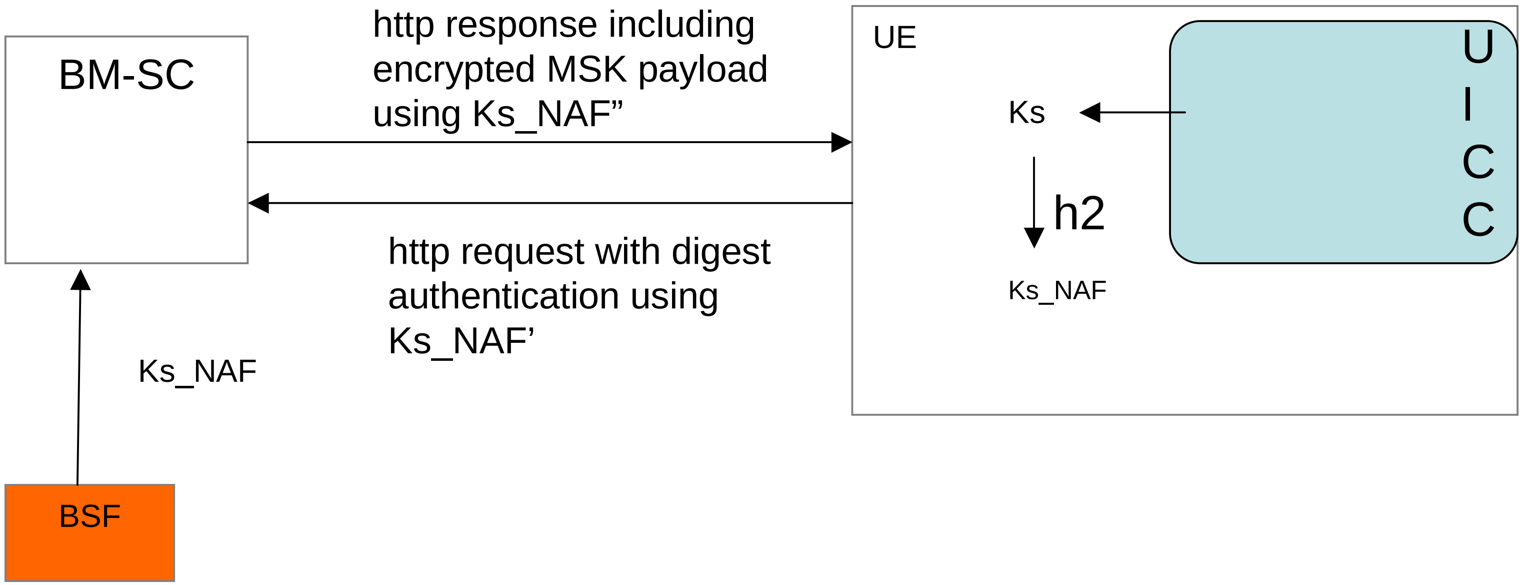
- Next slides contain a GBA view on key derivation and can be related to the scenarios of slide 7 and 8

UICC is GBA unaware (So has no MBMS application)


BM-SC
http response including encrypted MSK payload using Ks_NAF”
http request with digest authentication using Ks_NAF’
UE
Ks
h2
Ks_NAF
U I C C
Ks_NAF
BSF

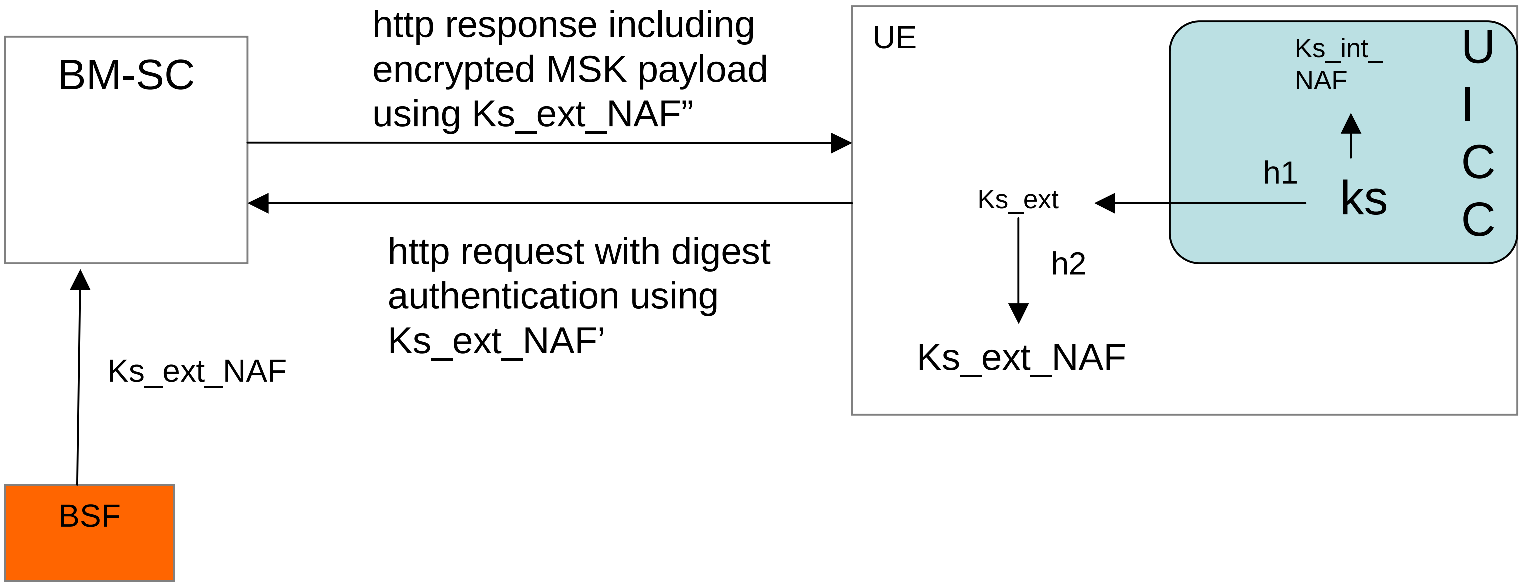
- This is based on GBA as specified within TS 33.220 v6.0.0
- The above figure uses http procedures as an example flow (not yet decided)
- The BM-SC may perform subsequent key derivation starting from Ks_NAF
- If the UICC supports an MBMS application then the UICC shall be GBA-aware
- This relates to Scn-1.

ME based MBMS key Management (scn1b)


BM-SC
http response including encrypted MSK payload using Ks_NAF”
http request with digest authentication using Ks_NAF’
Ks_NAF
BSF
UE
Ks
h2
Ks_NAF
U
I
C
C

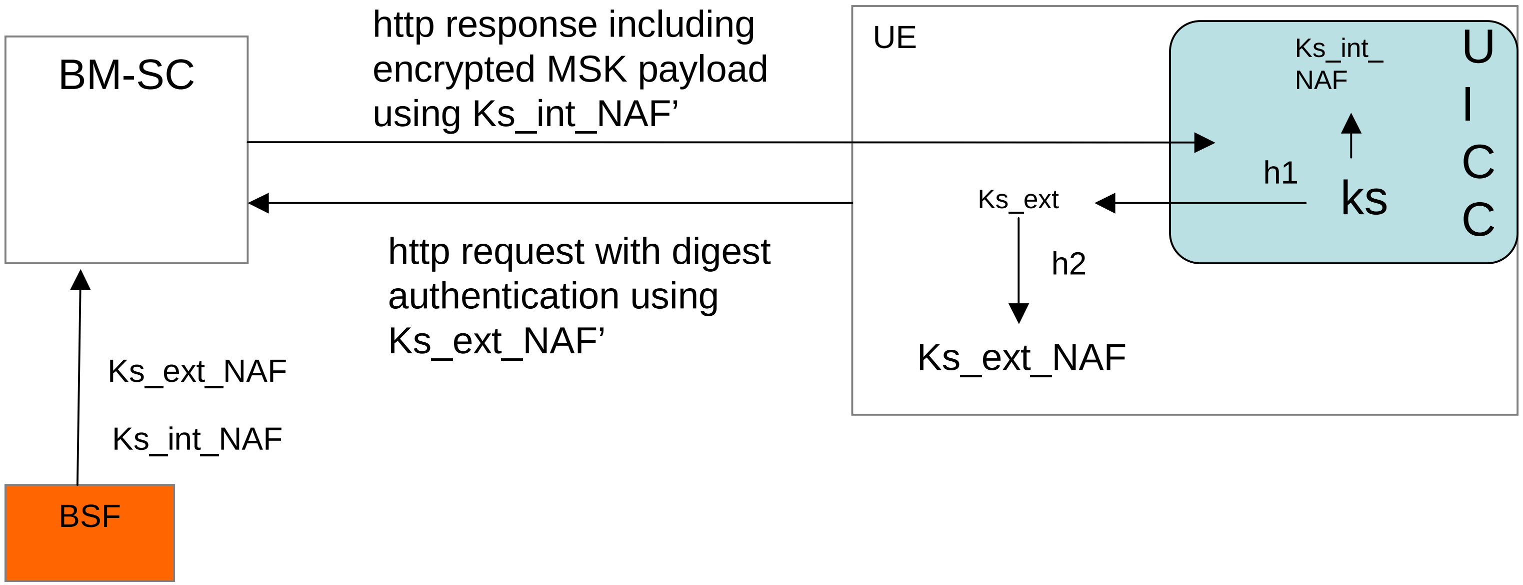
- This is based on GBA as specified within TS 33.220 v6.0.0
- As the network does not support GBA_U, the special-RAND flag is not set, so not GBA_U run is performed.

ME based MBMS key Management (scn1c)


BM-SC
http response including encrypted MSK payload using Ks_ext_NAF”
UE
Ks_int_NAF
U
I
C
C
h1
ks
Ks_ext
h2
Ks_ext_NAF
http request with digest authentication using Ks_ext_NAF’
Ks_ext_NAF
BSF

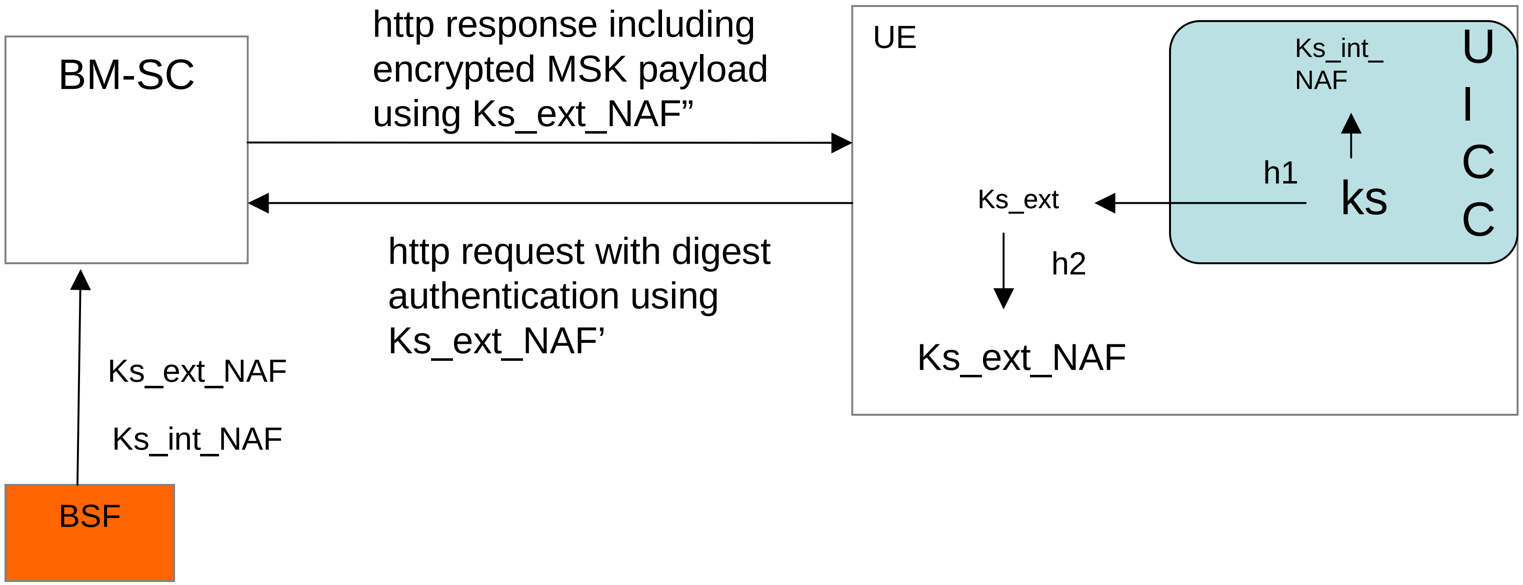
- The BM-SC may perform application specific key derivation
- As the Home Network supports GBA_U, the special-RAND flag is set, so GBA_U run is performed
- The key Ks_int_NAF is not delivered to the BM-SC as it does not support GBA_U

UICC based MBMS key Management


BM-SC
http response including encrypted MSK payload using Ks_int_NAF'
http request with digest authentication using Ks_ext_NAF'
UE
Ks_int_ NAF
U I C C
h1
ks
Ks_ext
h2
Ks_ext_NAF
Ks_ext_NAF
Ks_int_NAF
BSF

- The BM-SC may perform application specific key derivation
- Relates to Scn-2

ME based MBMS key Management


BM-SC
http response including encrypted MSK payload using Ks_ext_NAF"
http request with digest authentication using Ks_ext_NAF'
Ks_ext_NAF
Ks_int_NAF
BSF
UE
Ks_int_
NAF
h1
ks
UICC
Ks_ext
h2
Ks_ext_NAF

- The BM-SC may perform application specific key derivation
- Relates to scn-1d

Extra notes

- It is possible that an ME does support GBA_U procedures but no MBMS key management interfaces procedures. (in case also other UICC service will build on top of GBA aware UICC).
- In order to apply the right key management the BM-SC shall be able to know the UE capabilities for MBMS (i.e. support of ME or UICC key management).
  - This is a task of the MBMS User Service Joining Phase.
- The Rel-6 ME shall be able to detect if MBMS key management is supported by the UICC.