S3-040575

GBA_ME/GBA_U scenarios in UE att S3-040536

COMMENTED/REVISED BY AXALTO

July 1, 2004

Discussion

Reasoning:

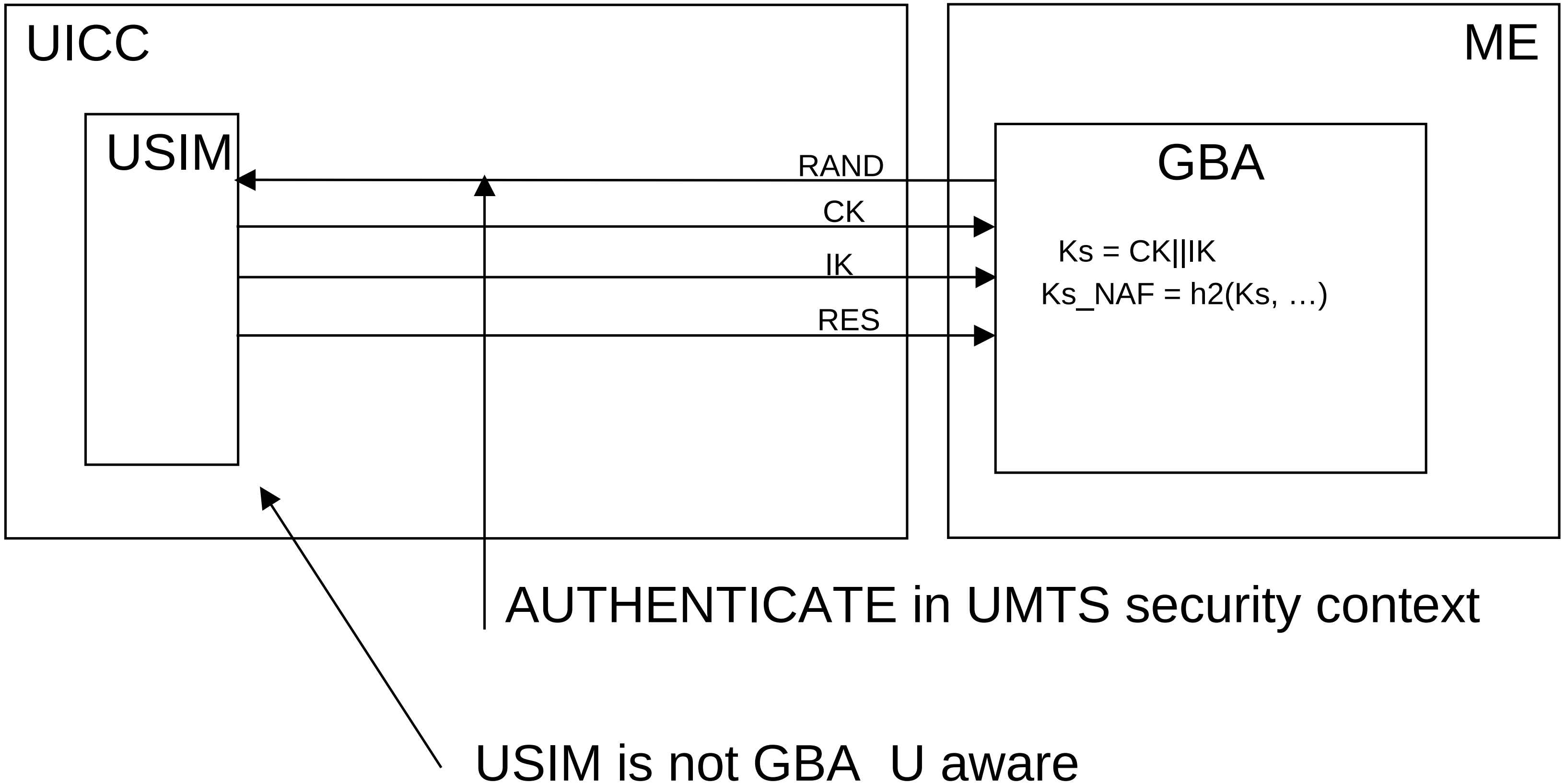
- Clarify key derivation
- Harmonize key derivation between GBA_ME and GBA_U
- All GBA ME shall be GBA_U aware

GBA_U functionality in the UICC can be (this is T3 issue):

- A new GBA_U security context of AUTHENTICATE command (as approved for VGCS)
- GBA_U capabilities will be announced in USIM/ISIM service table.

Following slides describe the procedures between different components when UICC application is either GBA_U aware or not.

GBA_ME



UICC

USIM

ME

GBA

RAND

CK

IK

RES

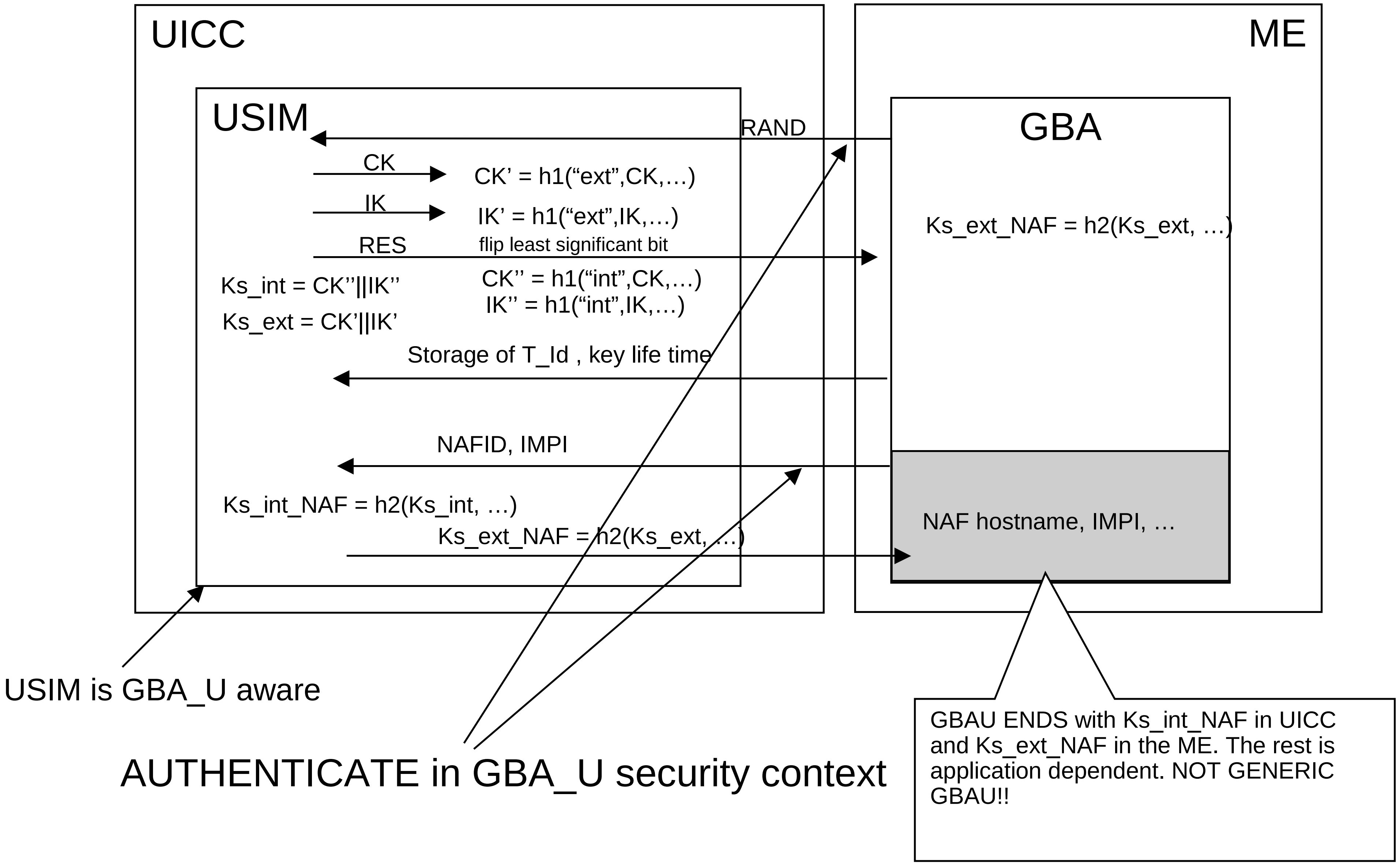
Ks = CK||IK

Ks_NAF = h2(Ks, …)

AUTHENTICATE in UMTS security context

USIM is not GBA_U aware

GBA_U USIM (with GBA_U AV)



UICC

USIM

RAND

CK

CK’ = h1(“ext”,CK,…)

IK

IK’ = h1(“ext”,IK,…)

RES

flip least significant bit

Ks_int = CK’’||IK’’

CK’’ = h1(“int”,CK,…)

IK’’ = h1(“int”,IK,…)

Ks_ext = CK’||IK’

Storage of T_Id , key life time

NAFID, IMPI

Ks_int_NAF = h2(Ks_int, …)

Ks_ext_NAF = h2(Ks_ext, …)

ME

GBA

Ks_ext_NAF = h2(Ks_ext, …)

NAF hostname, IMPI, …

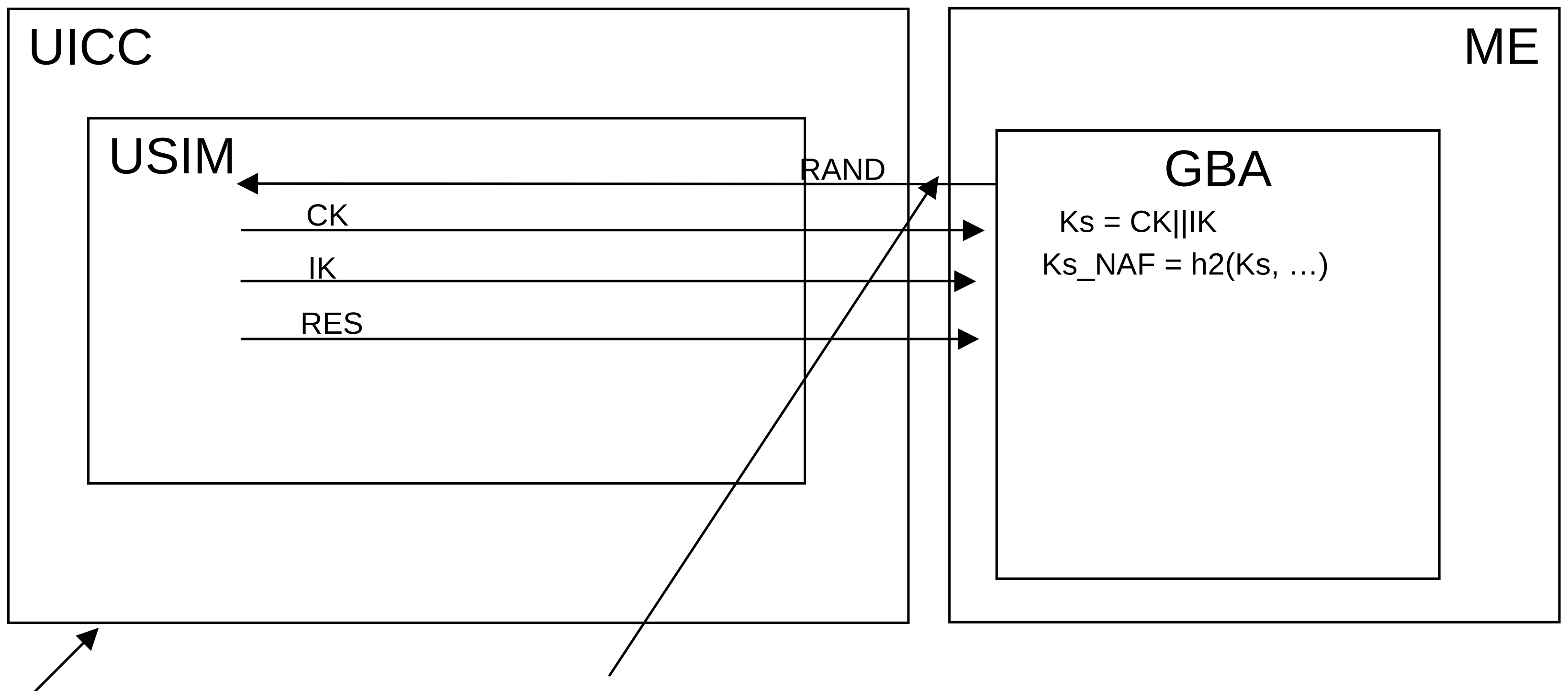
USIM is GBA_U aware

AUTHENTICATE in GBA_U security context

GBAU ENDS with Ks_int_NAF in UICC and Ks_ext_NAF in the ME. The rest is application dependent. NOT GENERIC GBAU!!

GBA_U USIM (with non GBA_U AV)

this scenario is needed if BSF does not support GBA_U AV retrieval/generation
This is however not suitable. BSF should send GBA_U AV to USIM GBA_U capable
(based in subscription information) (from the NAF perspective Ks_ext_NAF = Ks_NAF)
see S3-040475 / 6



UICC

USIM

RAND

CK

IK

RES

ME

GBA

Ks = CK||IK

Ks_NAF = h2(Ks, …)

USIM is GBA_U aware

AUTHENTICATE in GBA_U security context

Conclusions

- There are no advantages in not supporting GBA_U.
- The cost/implementation work for implementing GBA_U is minimal if ME support GBA_ME. (storage of B-TID + Key Life time and a second call for Ks_ext_NAF and Ks_int_NAF generation)
- Last scenario (slide 5) could be avoided if GBA_U AV modification is done at BSF level.
- GBA ME shall support both GBA_ME and GBA_U UICC interfaces.