Source: **3, Ericsson, Siemens**

Title: **ID handling Proposal**

Document for: **Discussion and Decision**

Agenda Item: **MBMS**

1 Proposal for ID handling in MIKEY

1.1 Design guidelines

General:

It has been attempted to keep the MSK and MTK messages as similar as possible.

For MSK delivery

For MSK delivery there is no need to optimize mikey Message length (at the cost of added complexity). This is not so much a problem as these messages are sent a lot less frequently than MTK messages. All the proposals to shorten the MSK message (via. MUK ID) introduced their own complexity, which was not felt worthwhile.

The choice of identities allows use of HTTP Digest in MBMS that fit well with Presence but without the TLS. Hopefully this will lead to easier standardisation in MBMS.

MRK-ID = B-TID – aligns with using Digest in Presence

MUK-ID = B-TID in BM-SC – aligns with MRK so no extra parameters to store in BM-SC

MUK-ID = identified by B-TID and NAF-ID combination in UE – this exactly aligns with GBA_U

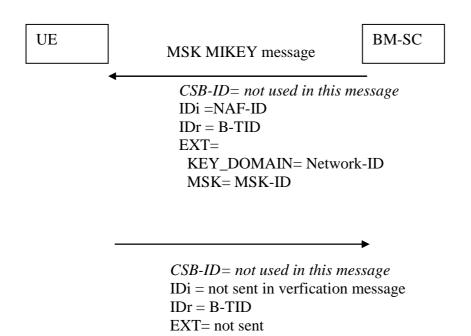*Notes on the use of The Network-ID (Call it Key domain ID ?)*

Network-ID has the same functionality as before (it could be renamed to Key Domain-ID; and add domain type in service announcement ?), but is now free for a service provider to populate, but it still needs to be globally unique. A mobile operator could (should) still use MCC||MNC, and a non-mobile operator could choose its own identity, as long as it is globally unique. The exact formatting is FFS. One possibility is to add this in the general extension payload.

This still allows a non-mobile operator to include a unique Network-ID of their own, i.e. overall it is less tied to mobile networks.

For MTK delivery

A small MTK message length is envisaged

1.2 Flows

```
┌──────────┐                                      ┌──────────┐
│   UE     │         MSK MIKEY message            │  BM-SC   │
└──────────┘ ◄─────────────────────────────────── └──────────┘
```

CSB-ID= not used in this message
IDi =NAF-ID
IDr = B-TID
EXT=
  KEY_DOMAIN= Network-ID
  MSK= MSK-ID

```
  ───────────────────────────────────►
```

CSB-ID= not used in this message
IDi = not sent in verfication message
IDr = B-TID
EXT= not sent

```
    ┌──────────┐                                      ┌──────────┐
    │   UE     │          MTK MIKEY message           │  BM-SC   │
    └──────────┘ ◄─────────────────────────────────── └──────────┘
```

CSB-ID=not used
IDi = not used in this message
IDr = not used in this message
EXT=
  KEY_DOMAIN= Network-ID
  MSK= MSK-ID
  MTK= MTK-ID