The Key ID Information Type for the General Extension Payload in MIKEY

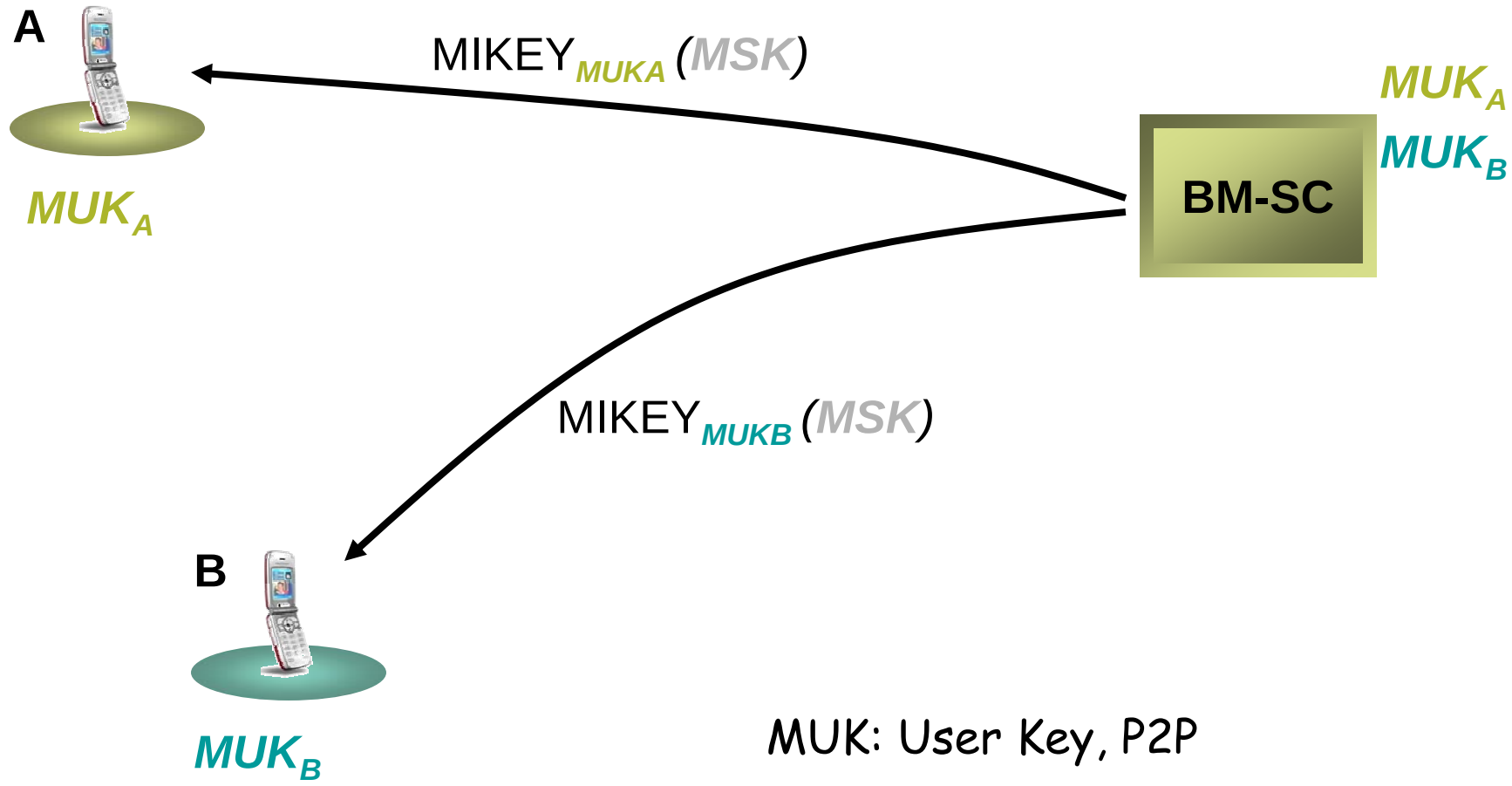
draft-carrara-newtype-keyid-00.txt

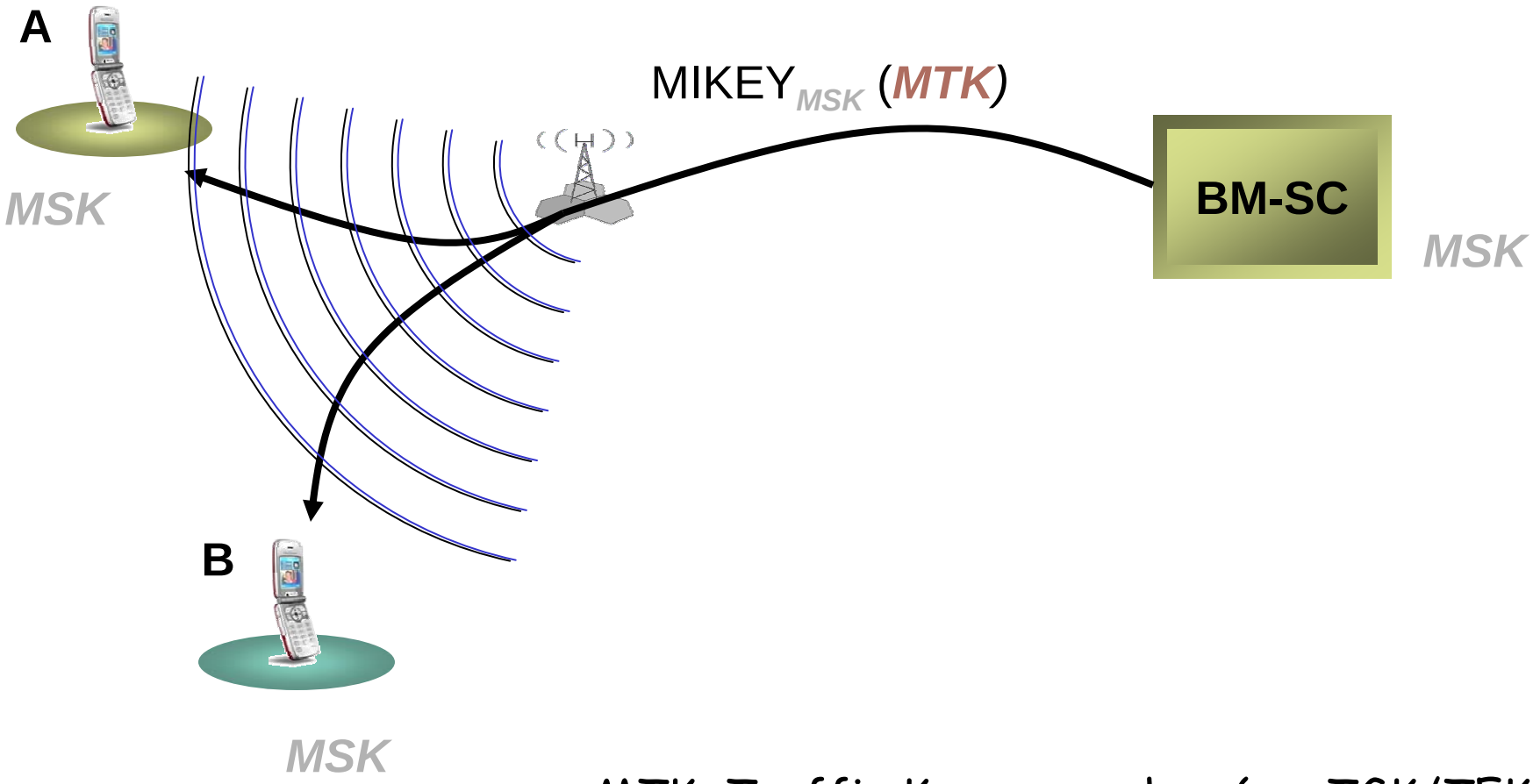
Objective

- Define a new type in the General Extension Payload in MIKEY needed by MBMS
- MBMS: Multimedia Broadcast/Multicast Service in 3GPP (Rel6)
  - functional freeze in December 2004
- The Streaming Scenario uses
  - SRTP for media protection
  - MIKEY for key mngt protocol
- MBMS requires to identify key type involved in the MIKEY message, and key identity

MBMS

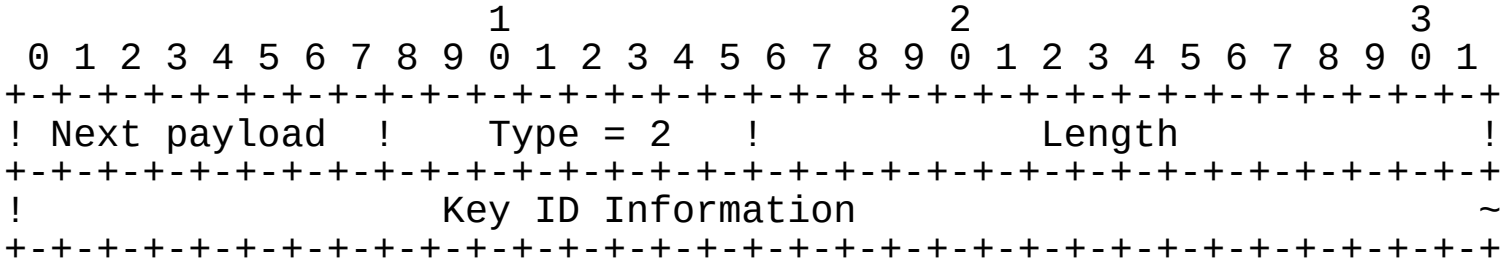
- Req: frequent key updates
  - Subscribers' inconveniency to publish decryption keys
- 3-level key mngt
  - Peer-to-peer key (MUK) *= shared secret*
  - Group key (MSK) *= KEK*
  - Traffic group key (MTK) *= TEK*
- Frequent MTK update


A
MIKEY MUKA (MSK)
MUK A
MUK A
MUK B
BM-SC
MIKEY MUKB (MSK)
B
MUK B
MUK: User Key, P2P
MSK: Service Key, group key

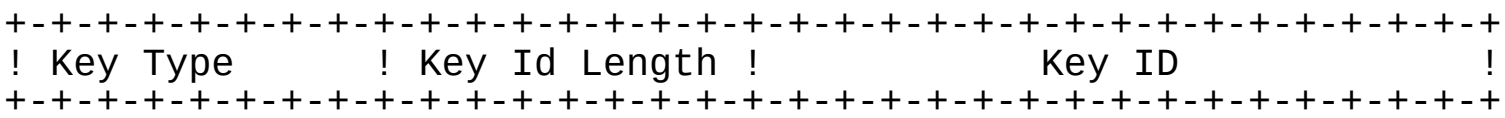


MTK: Traffic Key, group key (eq. TGK/TEK)

General Extension Payload in MIKEY



Key ID Information:



Key Type	Value
MBMS User Key (MUK)	0
MBMS Service Key (MSK)	1
MBMS Transport Key (MTK)	2