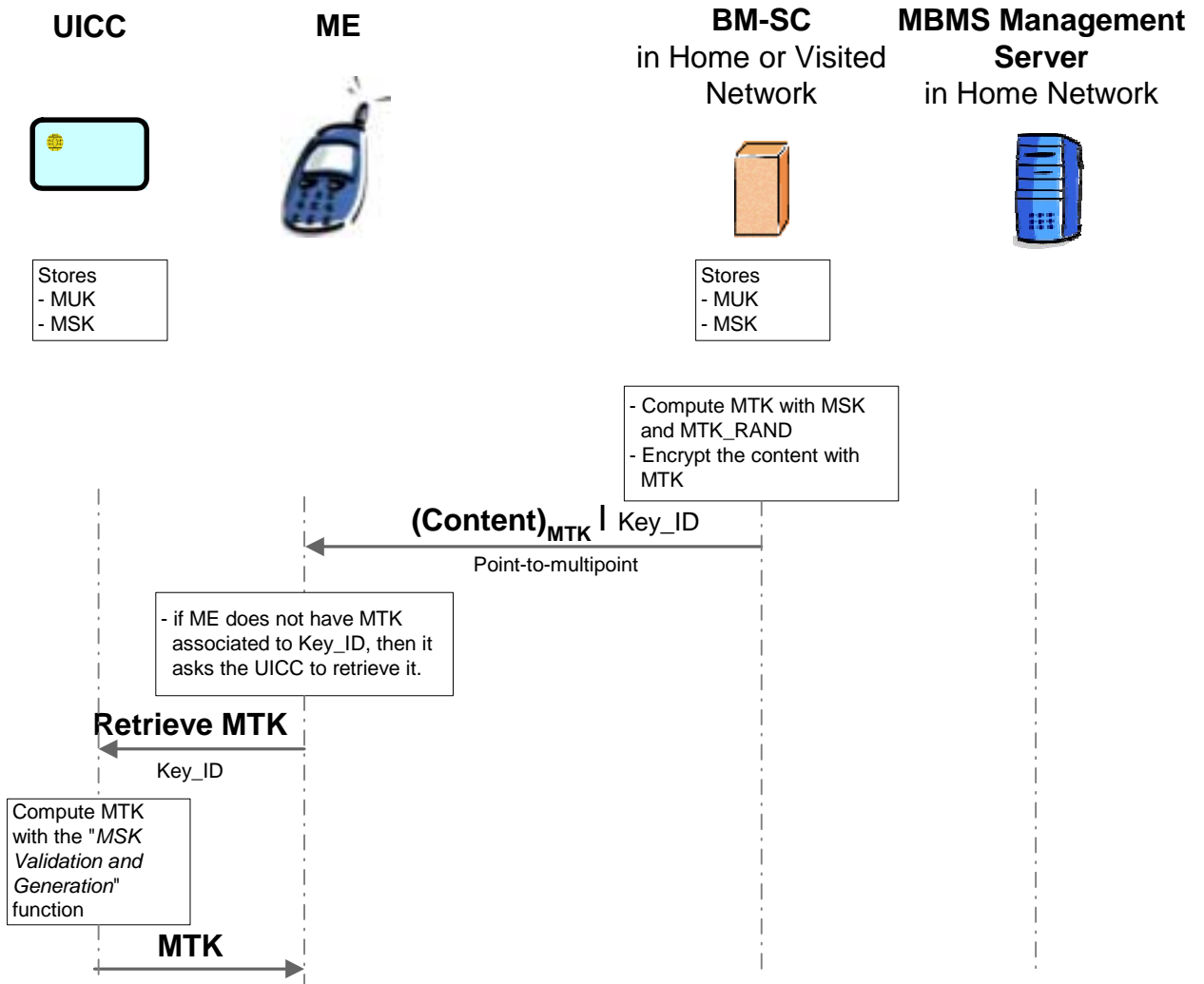|	
Source:	**Oberthur Card System – commented by Siemens 21/4/2004**
Title:	**MBMS Pay per view charging model**
Document for:	**Discussion**
Agenda Item:	**6.20**

Abstract

This contribution describes a way of implementing a charging model for MBMS UICC-based only solution allowing pre-paid and post paid access to content on a pay-per-view basis.

1. Introduction

At SA3#32, questions about latencies in the system and the need for instant access to a content have come up. This contribution aims at proposing a solution in the context of the MBMS OTA-based system. It also proposes different charging schemes based on a purse system, either pre-paid or post-paid. As a by-product, it allows for an easy solution for instant access to content.

2. Overview of the solution

2.1. MBMS Operating procedure

UICC

ME

BM-SC
in Home or Visited
Network

**MBMS Management
Server**
in Home Network

Stores
- MUK
- MSK

Stores
- MUK
- MSK

- Compute MTK with MSK
  and MTK_RAND
- Encrypt the content with
  MTK

(Content)$_{MTK}$ | Key_ID

Point-to-multipoint

- if ME does not have MTK
  associated to Key_ID, then it
  asks the UICC to retrieve it.

Retrieve MTK

Key_ID

Compute MTK
with the "*MSK
Validation and
Generation*"
function

MTK

2.2. Associating several MSK's to the same content

When a content is sent to the ME, the Key_ID field may be set-up so that several MSK's may be used to decrypt the MTK (the exact formatting is ffs). This is possible as long as the algorithms used to produce the MTK are reversible, which is the case if 3DES or AES are used.

The ME sends the Key_ID field to the IUCC in the Retrieve_MTK command, the UICC then processes the list of MSK's and checks whether any of the MSK's is stored in one of the MBMS Keysets.

2.3. Pay per view specific keys

Amongst the MSK_ID's in the list contained in the Key_ID field, there may be one or several MSK's associated with a Pay per view scheme. In this case, each usage of this specific MSK to decrypt a MTK will decrement the purse in a pre-paid scheme, alternatively increment the purse in a post-paid scheme.

The details of purse management are for further study.

2.4. Immediate access to content

Clearly, a purse based pay per view scheme does allow immediate access to any content that has the corresponding MSK info in the Key_ID field.

In the case where the purse is used to cover an operational delay for the updating of the Keyset, the initial expense may be later on redeemed; this is ffs.

3. Conclusion

The MBMS UICC-based only solution, based on existing 3GPP infrastructure, offers a simple possibility to provide services using pre-paid or post-paid models of charging for the access to MBMS broadcasted content.

Should SA3 confirm its interest in this issue and decide to endorse this approach, we propose to prepare specifications.