

Source: Gemplus, Oberthur, QUALCOMM Europe, SchlumbergerSema
Title: MBMS Usage and Quality of Service based on BAK Distribution
Document for: Discussion
Agenda Item: MBMS

1. Introduction

Operators have expressed the desire to have usage-based billing for MBMS at a level of finer granularity than the BAK subscription periods allow. One approach would be to get the terminal (ME) to report how much time the user spent accessing the content. The terminal should not be trusted to report accurately.

In this document we outline a secure mechanism for determining usage that may be layered on top of the BAK proposal, because it is UICC-based. The scheme is based on the UICC counting the number of SK values generated and reporting these values to the network as required, and using MBMSManagementOperations to convey this information. This scheme can also be very useful for evaluating quality of service or otherwise measuring what content individual users are accessing.

2. More details

The SK counters would be stored on the UICC. The SK counter would be associated with a particular MBMS service, although that counter could be allocated to families of MBMS services to save space or for marketing and commercial reasons. When a BAK is provisioned onto the UICC, and the operator wants to count the SK values for this MBMS service, then there will be a corresponding MBMSManagementOperation indicating to the UICC to count the number of SK values generated for that service.

The SK counters would only be reset securely. The network determine usage over a particular time period by requesting the values of the appropriate SK counter at the beginning and end of the time period: the usage is determined by calculating the difference.

From a security perspective there are two important aspects to performing SK counting.

- It is important that the UICC attach integrity protection to ensure that the value of the SK counter is not changed in transit between the UICC and the network.
- It is important that only appropriate network entities can authorize the UICC to allocate new MBMS services to a particular SK counter. Otherwise, it is to the user's advantage to send fake authorizations of this kind to the UICC, resulting in usage information being lost.

Detailed security mechanisms are being addressed in [1].

[1] USIM Enhancements for MBMS Support, S3z030009