3GPP TSG SA WG3 Security — SA3#35 **S3-040815**

October 5-8, 2004

St Paul's Bay, Malta

Title: **Initiation of key management in MBMS**

Source: **Ericsson**

Document for: **Discussion and decision**

Agenda Item:

Work Item: **MBMS**

1 Introduction

In MBMS security joint meeting between SA3 and SA4 in August 2004 it was noted by SA4 delegates that SA4 does not currently see a need for Application level joining, i.e. from SA4 point of view there seems to be no need for application level signaling between UE and BM-SC to initiate a User Service. However, from SA3 point of view there is a need to be able to initiate key management for the MBMS User Service. This could be done based on the security information in the Service Announcement/ Discovery procedure that is defined as a part of TS 26.346 [1] in SA4.

This contribution and accompanying CR describe which security parameters are needed in the Service Announcement/ Discovery and how UE will request the initiation of key management.

2 Description

2.1 Security parameters in Service Announcement/ Discovery

The TS 26.346 v1.0.0 specifies the following clause 5.2.1:

User service discovery refers to methods for the UE to obtain a list of available MBMS user services along with information on the user services. Part of the information may be presented to the user to enable service selection.

User service announcement refers to methods for the MBMS service provider to announce the list of available MBMS user services, along with information on the user service, to the UE.

In order for the user to be able to initiate a particular service, the UE needs certain metadata information. The required metadata information is described in section 5.3.

Regarding the parameters clause 5.3 says currently:

[Service type: streaming, messaging etc. (to launch the right application in the terminal)];
[broadcast or multicast mode];
[security on/off and related parameters];
[user service session start/stop time];
[Port #, IP@, protocol];

[media types and codecs];
[QoS, data rates, UE MBMS bearer capability requirements, etc.];
[FEC on/off, related parameters];
[session identification];
[content delivery verification on/off and related parameters]

The following security parameters are proposed to be included in the User Service Announcement in TS 26.346:

- **Confidentiality protection: on / off**.

- **Integrity protection: on / off**

- **Network address of the key management server**: I.e. the address of the BM-SC, e.g. in the form of URI.

- **List of keys needed to receive the service**: The keys should include the identifiers of the Key Groups that are needed for the user service. The Key Groups are identified as specified in TS 33.246, i.e. as a concatenation of Network ID and Key Group ID. Note that the MSK ID or MTK ID is not needed since they are sequence numbers and are changing over time. E.g.

    - Key-IDx: [Network ID: xx, Key group ID:];

    - Key-IDy: [Network ID: xx, Key group ID:]

- **Mapping of MSKs to the delivered entities**: The MSKs need to be mapped to the delivered entities, e.g. transport services so that the UE knows what keys are used to protect which stream. E.g.

    - Map: [Key-IDx -> IP@];

    - Map: [Key-IDy -> IP@]

2.2 Initiating the key management

When the UE receives the Service Announcement/ Discovery information, it initiates the key management if the human user decides to join this user service. The UE fetches the keys needed from the BM-SC. The UE will do the following:

1. The UE receives the Service Announcement/ Discovery information

2. If the human user decides to join this user service, the UE sends the HTTP request message to the network address indicated (i.e. BM-SC) and requests for the keys that were indicated in the announcement.

    - Key-IDx: [Network ID: xx, Key group ID: xy];

    - Key-IDy: [Network ID: xx, Key group ID: yy]

3. The BM-SC consults the BSF for GBA keys, if needed, and mutual authentication with HTTP digest takes place. The BM-SC makes authorization checks for the UE and responses with success or failure.

4. If the UE was authorized, the BM-SC starts to push MIKEY key management messages to the UE.

3 Conclusions and proposal

The contribution has shown how key management is initiated based on the information in the Service Announcement. It is important that the correct Service Announcement/ Discovery information is in place. It is proposed to approve the accompanying CR, which implements this in the TS 33.246 [2].

4 References

[1] TS 26.346, MBMS; Protocols and codecs

[2] TS 33.246, Security of MBMS