3GPP TSG SA WG3 Security — SA3#35 **S3-040808**

October 5-8, 2004

St Paul's Bay, Malta

Title: **MBMS security work split**

Source: **Ericsson**

Document for: **Discussion and decision**

Agenda Item:

Work Item: **MBMS**

1 Introduction

The MBMS security work in SA3 is related to the MBMS work being done in work groups SA4 and CN1. CN1 has the responsibility to define the stage 3 details of Ua interface between the UE and BM-SC. Functionality in SA4 related to security are e.g. Key fetching, Service Announcement and Post delivery procedures (such as point to point repair).

This contribution discusses the security related work in CN1 and SA4 and proposes how the specification work could be distributed between the work groups.

2 Discussion

2.1 Work between CN1 and SA3

2.1.1 User authentication and key management

WG CN1 has a TS 24.109 [2] that specifies the stage 3 of Ub and Ua interfaces. TS 24.109 defines e.g. the stage 3 details of HTTP digest authentication over Ua.

SA3 has agreed to use HTTP digest using GBA secret for user authentication over Ua. Therefore it would be natural that stage 3 of MBMS user authentication with HTTP digest is specified in 24.109. On MBMS Key management, SA3 has made detailed work based on MIKEY protocol. This work is regarded to be at Stage 3 level and, thus does not seem to require additional work in CN1. This work split issue between user authentication and key management was discussed in CN1#35 in contribution [1], which was agreed.

Now, what remains between SA3 and CN1 responsibility are the key management parameters that are needed in HTTP request and response messages over Ua. The following work split is proposed between the groups:

- the key management parameters in HTTP messages are defined in TS 33.246 with hints of length where possible, and
- TS 24.109 specifies the detailed HTTP procedures and how these parameters are formatted

It is proposed that the parameters would be formatted as an XML schema that could be placed in a normative Annex in TS 24.109. Similar normative Annex has already been done in TS 24.109 as Annex C for carrying "bootstrapping key lifetime". A MIME type needs to be registered for the MBMS XML schema.

2.1.2 Application layer joining

In the MBMS security joint meeting between SA3 and SA4 it was noted that SA4 has not made a decision on the need for application layer joining. However, it was also noted in the meeting that SA3 needs a procedure over Ua to initiate key management between UE and the BM-SC. This procedure could be seen as an "application layer joining" and SA4 might later include parameters to it if they see need for it. It is proposed that this initial key management is handled in the same way as the key management above.

2.2 Work between SA4 and SA3

It should be noted that SA4 has done stage 3 level work on their procedures and therefore the need for CN1 involvement should be discussed between SA4 and CN1. In order to have a complete view on Ua interface procedures CN1 TS 24.109 could include the SA4 procedures and refer to SA4 TS for details. The chapters below specify what could be the work split between SA3 and SA4.

2.2.1 Service Discovery/Announcement

SA4 specifies in TS 26.346 [3] User Service Discovery/Announcement procedures, which should include also security parameters, e.g. needed keys for the service. SA3 should give input to SA4 what security parameters are needed in Service Discovery/Announcement. SA4 intends to specify the Service Discovery/Announcement in XML format. Similarly as in CN1 case above it is proposed that

- the security parameters in Service Discovery/Announcement are defined in TS 33.246 with hints of length where possible, and
- TS 26.346 specifies how these parameters are formatted. It may be natural to specify the parameters in XML format

2.2.2 Post delivery procedures

SA4 specifies so called post delivery procedures, e.g. point to point repair, in TS 26.346. SA4 will use HTTP as transport and SA3 has specified to use HTTP digest to secure the transport. In the MBMS security joint meeting between SA3 and SA4 it was noted that SA4 post delivery procedures are somewhat immature to be able to specify the exact protection method and that it would be desirable to have a common framework for all post delivery procedures that could then be protected in a consistent way by SA3. It is proposed that SA4 develops the post delivery procedures further before SA3 defines the protection methods.

2.2.3 Traffic protection mechanisms

As SA4 is traditionally responsible for the transport protocols, it is proposed that the MBMS Traffic protection details are handled between SA3 and SA4.

3 Conclusions and proposal

.The proposal is summarised in the table. It is also proposed to send an LS to both SA4 and CN1 on the proposed work split and ask for their opinion on the issue. Due to the limited time schedule in Rel-6 it is

recommended that interested companies should raise these coordination issues as company contributions in respective working groups.

The work split is proposed in the following table:

Procedure	Protocol	High level description	Detailed description
Service Announcement/Discovery	N/A	SA3 specifies what security parameters are needed.	SA4 specifies how the security parameters are allocated in Service Ann./Disc, e.g. in XML schema
Initial key management ("application level joining")	HTTP	SA3 specifies what security parameters are needed (SA4 TS may include some procedures for complete view)	CN1 specifies how the security parameters are allocated, e.g. in XML schema
Pull key request	HTTP	SA3 (SA4 for complete view)	CN1 specifies how the security parameters are allocated, e.g. in XML schema
Push key procedures	MIKEY	SA4 TS may include some procedures for complete view	SA3 specifies details of MIKEY No CN1 involvement
Data delivery	(S)RTP / FLUTE	N.A.	SA3 for security parameter handling SA4 for data transport protocols non-security details No CN1 involvement
Post delivery	HTTP	SA3 specifies what security parameters are needed (SA4 TS includes the procedure overview)	CN1 specifies how the security parameters are allocated, e.g. in XML schema. SA4 specifies transport non-security details

4 References

[1] TD N1-041397, MBMS Security work

[2] TS 24.109, Bootstrapping interface Ub and Network application function interface Ua

[3] TS 26.346, MBMS; Protocols and codecs