3GPP TSG SA WG3 Security ó SA3#35 **S3-040847**

October 5-8, 2004

St Paul's Bay, Malta

Title: **Finalization of MBMS security work**

Source: **Ericsson, Nokia, Siemens**

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, Post delivery procedures (such as point to point repair) and the Traffic Protection (such as encryption).

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

2 Discussion

2.1 Where to finalise MBMS security work?

As noted above, three work groups could be involved in finalising MBMS security work. However, it is proposed that only SA3 and SA4 are involved. This is due to the following reasons:

- The deadline for Rel-6 is approaching.
- There will be one group less in the specification work, which means less coordination and more efficient specification work.
- There will be one specification less that handles MBMS. Therefore the risk of confusion or contradicting specifications is smaller.
- CN1 does not have a specific TS for MBMS, thus there is no need to create a new TS.
- SA4 procedures are closely related to security, and SA4 has already done stage 3 level work on those procedures.

It could be noted that CN1 TS 24.109 [1] includes stage-3 description for user authentication in PKI enrolment over Ua reference point (i.e. between UE and application server). For consistency reasons stage-3 user authentication in MBMS could also be described in that TS. It should be noted that CN1 has discussed this issue in [6] and CN1 agreed to specify stage-3 user authentication for MBMS in TS 24.109. However, considering the arguments listed above this is not recommended. Therefore it is proposed that only SA3 and SA4 are involved in finalising MBMS security work.

2.2 How to finalise MBMS security work?

The below subchapters describe how the work should be coordinated between SA3 and SA4 on the following areas:

- Service Discovery/Announcement
- Key management procedures with HTTP (e.g. initialisation of key management)
- Key management procedures with MIKEY
- Post delivery procedures
- Traffic protection mechanisms

2.2.1 Service Discovery/Announcement

SA4 specifies in TS 26.346 [3] User Service Discovery/Announcement procedures. The Service Description sent to the user should include also security parameters, e.g. needed keys for the service, so that the user can initiate key management. SA3 should give input to SA4 what security parameters are needed in Service Discovery/Announcement. It is assumed based on TS 26.346 that SA4 intends to specify the Service Discovery/Announcement in XML format. It is proposed that

- the needed security parameters in Service Discovery/Announcement are defined by SA3 in TS 33.246 [2]
- TS 26.346 specifies in detail (stage-3) how these parameters are formatted in XML in Service Description.

The information transfer from SA3 (stage-2) to SA4 (stage-3) should be performed via company contributions.

2.2.2 Key management procedures with HTTP

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 to initiate key management between UE and the BM-SC. It was also noted that this ìinitial key managementî procedure could be seen as an ìapplication layer joiningî and SA4 might later include parameters to it if SA4 see need for it. This initial key management is triggered, if the user has decided to join the service advertised in the service announcement.

SA3 has agreed that the UE shall use HTTP for requesting MBMS keys from the BM-SC. The UE may request the keys in the beginning of the service to initiate the key management or during the service if he has missed a key update. SA3 has also agreed that HTTP messages are authenticated and integrity protected using HTTP digest headers. The needed shared secret for HTTP digest is received from bootstrapping procedure, which is described in TS 33.220[4].

It is proposed to coordinate the work on HTTP based key management in the following way:

- SA3 specifies in TS 33.246 what parameters are needed in the HTTP request and response messages for requesting the keys and how these parameters are used. The parameters should be carried in the client/server payloads in HTTP messages.

- SA4 specifies in TS 26.346 in detail how these parameters are carried in client/server payloads. It is proposed that the parameters are formatted as an XML schema. MIME type(s) needs to be registered for the XML schema for the client/server payloads.

The information transfer from SA3 (stage-2) to SA4 (stage-3) should be performed via company contributions.

2.2.3 Key management procedures with MIKEY

MBMS key management consists of two building blocks, where HTTP request/response procedure is used to request keys and the actual key delivery is performed with a separate procedure using MIKEY protocol [5]. It should be noted that SA3 has made detailed work based on MIKEY protocol. This work is regarded to be at stage-3 level and, thus does not require additional work in SA4.

2.2.4 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 tentatively 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.

2.2.5 Traffic protection mechanisms

As SA4 is traditionally responsible for the transport protocols, it is proposed that SA4 defines the transport and SA3 defines how to secure the transport.

3 Conclusions and proposal

This contribution has discussed the finalisation of MBMS security.

- It is proposed that MBMS security work should be finalised in cooperation between SA3 and SA4 and that CN1 is not involved.

- It is also proposed how the security work should be finalised. This is described in chapter 2.2.

- Due to the limited time schedule in Rel-6 it is recommended that the information transfer from SA3 to SA4 for the topics mentioned above is handled via company contributions

It is also proposed to send an LS to both SA4 and CN1 on the issue.

The proposed work coordination is 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
HTTP key request and response	HTTP	SA3 specifies what security parameters are needed in the HTTP request and response messages and how these parameters are used (SA4 TS may include some procedures for complete view)	SA4 specifies how the security parameters are allocated in XML schema.
MIKEY key delivery procedure	MIKEY	N.A.	SA3 specifies details of MIKEY
Data delivery	(S)RTP / FLUTE	N.A.	SA3 for security parameter handling SA4 for data transport protocols non-security details
Post delivery procedures	HTTP	SA4 specifies the procedure. SA3 specifies what security parameters are needed	SA4 specifies how the security parameters are allocated

4 References

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

[2] TS 33.246, MBMS Security

[3] TS 26.346, MBMS; Protocols and codecs

[4] TS 33.220, Generic Bootstrapping Architecture

[5] IETF RFC 3830, MIKEY: Multimedia Internet Keying

[6] TD N1-041397, MBMS Security work

3GPP TSG SA WG3 Security ó SA3#35 **S3-040xxx**
October 5-8, 2004
St Paul's Bay, Malta

Title:	Draft LS on MBMS Security finalisation
Response to:	
Release:	Rel-6
Work Item:	MBMS
Source:	SA3
To:	CN1, SA4
Cc:	

Contact Person:

Name:	Vesa Lehtovirta
Tel. Number:	+358 40 509 3314
E-mail Address:	Vesa.Lehtovirta@ericsson.com

Attachments:	S3-040xxx

1. Overall Description

In meeting SA3#35, 5 ñ 8 October 2004, SA3 has discussed TD S3-040xxx on how the work on MBMS security should be finalised in stage 2 and stage 3 in Rel-6.

SA3 has also noted that CN1 has discussed this issue in TD N1-041397 [1]. However, SA3 has come to the conclusion that MBMS security work in Rel-6 should be finalised by SA3 and SA4. No CN1 involvement is required.

The reasons to concentrate the MBMS security work to SA3 and SA4 are:

- The deadline for Rel-6 is approaching.
- There will be one group less in the specification work, which means less coordination and more efficient specification work.
- There will be one specification less that handles MBMS. Therefore the risk of confusion or contradicting specifications is smaller.
- CN1 does not have a specific TS for MBMS, thus there is no need to create a new TS.
- SA4 procedures are closely related to security, and SA4 has already done stage 3 level work on those procedures.

How the work should be finalized between SA3 and SA4 is described in the attached contribution S3-040xxx. In principle, SA3 will provide a detailed description of the SA3 procedures, so that SA4 can do the actual stage 3. SA3 will do the stage 3 of the MIKEY messages.

To SA4 and CN1 group.

ACTION: SA3 kindly asks SA4 and CN1 to comment the SA3 view on MBMS security work finalisation.

3. Date of Next TSG-SA3 Meetings

SA3#36	23 - 26 November 2004	Shenzhen, China
SA3#37	21 - 25 February 2005	Sophia Antipolis, France

4. References

[1] TD N1-041397, MBMS Security work