3GPP TSG SA WG3 Security ó SA3#35 **S3-040884**
October 5-8, 2004
St Paul's Bay, Malta

Title:	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: S3-040847, Contribution: MBMS security work split
S3-040692, Report of MBMS joint Ad-hoc meeting

1. Overall Description

In meeting SA3#35, 5 ñ 8 October 2004, SA3 has discussed TD S3-040847 on how the work on MBMS security should be finalised in stage 2 and stage 3 in Rel-6.

SA3 has 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. Based on the reasons listed below it is proposed that CN1 would not be involved in finalising MBMS security.

- SA3 has noted that CN1 has been deeply involved in specifying MBMS Transport Service details, but has not been much involved in MBMS User Service work.

- User Service procedures in SA4 are closely related to security, and SA4 has already done stage 3 level work on those procedures.

- CN1 does not have a specific TS for MBMS User Services, thus there is no need to create a new TS.

- There will be one specification less that handles MBMS security. Therefore the risk of confusion or contradicting specifications is smaller.

- There will be one group less in the specification work, which means less coordination and more efficient specification work.

- The deadline for Rel-6 is approaching.

How the work should be finalized between SA3 and SA4 is described in the attached contribution TD S3-040847. In principle, SA3 would provide a detailed description of the SA3 procedures, so that SA4 could do the actual stage 3. SA3 will do the stage 3 of the MIKEY messages.

Due to the limited time there are not many possibilities to exchange liaison statements, therefore companies are encouraged to direct offline discussions to progress the work. It should be highlighted that SA3 and SA4 held a joint meeting in August 2004 on MBMS Security [2]. The participants of the joint meeting should be contacted.

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

[2] TD S3-040692, Report of MBMS joint Ad-hoc meeting

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

3GPP TSG SA WG3 & WG4 joint meeting **S3S4J040018**

23-24 August 2004

Sophia Antipolis, France

Source: **Chairman of 3GPP TSG-SA WG3**

Title: **Draft report of joint SA3-SA4 meeting on MBMS security**

Document for: **Approval**

1 Opening of the meeting (Monday, 23 August, 14:00)

2 Agreement of the agenda

The agenda was agreed.

It was agreed that the main meeting objective was for both groups to gain a better understanding of the work in each group. This would help identify gaps and overlaps in the two specifications and this information could then be used to complete the work in each group with the resulting specifications fitting together well. It was also hoped to draft some text for the SA4 specification, particularly the security section.

2.1 3GPP IPR Declaration

3 Assignment of input documents

4 Status of relevant specifications

4.1 SA3 specifications on MBMS

Tdoc 12 (MBMS security rapporteur) provides an overview of the work in the MBMS TS.

If there are two distinct RTP flows (either on one MBMS bearer with two ports or on two MBMS bearers), are there issues to using one MTK or two for this situation. What other effects are there on the keying procedures. The more complicated scenarios that are allowed, the more complicated it will be come to know when a MTK can be thrown away. It was commented that the SA3 specification did not currently contain a method of throwing away old MTKs.

The issue of updating MTK was raised. It was commented that for streaming MTKs could be updated by interleaving MIKEY messages in the RTP stream carrying the data. The error resilience of this was questioned. It was noted that the MTK messages could be repeated. It was observed that there is nothing about this possible repetition in the SA3 TS 33.246. It was also noted that the TS does not mention the port numbers used for using MIKEY over UDP. It was asked if it had been considered to have a separate point-to-multipoint channel for the delivery of MTKs. This had not been considered by SA3 but is possible, although it would bring its own complexities, e.g. the need for the UE to open the ptm bearer to listen for MTK updates. Before this could be accepted, it was felt that the trade-offs between the two solutions would need to be studied in detail.

The relationship between MTK and MKI (the Master Key Identifier field in SRTP) was raised. It was noted that it would be compulsory to include the MKI field in all STRP packets for MBMS. More study is needed to look if the MKI field (9 bytes currently) can be omitted in parts of the RTP trailer.

It was asked how does the BM-SC know which UEs to send the new MSKs to? This would be done by some registering of interest in the service by the UE, which from SA3 perspective relates to application layer joining. SA4 delegates indicated that there was no SA4 requirement for UE to contact BM-SC to receive MBMS services.

Tdoc 13 (SA3) is the latest version of the SA3 MBMS specification, TS 33.246.

It was noted that there needs to be a Unique Key Group ID across multiple BM-SCs. SA3’s specification needs to be adapted for this.

It was asked how the BM-SC could contact the UE to send an MSK update if the UE is in idle mode. In that case the user has no active PDP context (no IP address exists). It was asked whether a Gmb procedure existed for this. SA3 action to think about and contact the relevant group (CN3) ?

Similarly how does a UE know how to contact the BM-SC. This information could be contained in the User Service Description.

It was felt that some text showing how put an MBMS service together would be useful. This could be contained in the SA4 TS or TR. There was some concern about not having it in the TS, as it would not seem part of the technical specifications.

It was noted that SA3 solution is actually bearer agnostic such that the data can be transported in multicast mode as well as in broadcast mode. This was recognized as a possible reason for the application layer joining procedure.

4.2 SA4 specifications on MBMS

Tdoc 14 and **tdoc 15** (SA4) are the latest versions of TS 26.346 and TR 26.946.

Download section is quite mature while the Streaming section is less mature. Other sections still need more work.

The RTCP (in downlink) is automatically integrity protected by SRTP (called SRTCP).

There was a request from SA4 for input to clause 9 of the specifications.

There were doubts if the User Service Description needs to be integrity protected.

Tdoc 11 (Siemens) reviews the SA4 contribution S4-040527.

It was noted that document 527 has not been agreed by SA4-plenary. Still the joint meeting felt it usefull to discuss this early draft of reference architecture in order to get a mutual understanding of the allocation of security functions within it.

- Why Gmb proxy? The Gmb proxy is optional. The SA2 specification allows a split of Gmb functionality into the user authorisation and the Session Start like functionality that indicates data is about to be sent. The Gmb proxy is under discussion and if it part of the BM-SC it will require no standardisation and only be part of the Gmb interface.

- In clause 4.4, it was noted that some functions are not allocated to blocks in the architecture.

- The joint meeting agreed that it was important to add security functions in additions to the procedures given S4-040527. It was felt that the best way to achieve this was via company contributions directly to SA4.

- SA4 use the term User Service Initiation, whereas SA3 use the term application layer joining. SA3 should align with the SA4 terminology where appropriate. It was noted that it is currently not clear if the application layer joining would be a subprocedure of this User Service initiation or a separate procedure. The final specification of these procedures will need to be aligned between SA3, SA4 and CN1.

- There were other editorial changes discussed. An update of the document including the agreed changes was made in **tdoc 16** and can be used by SA4 for reaching argreement on appropriate text in their next meeting.

5 Questions from SA3 to SA4

5.1 Questions presented in the LS S3-040675

5.2 What is the SA4 status on MBMS application layer joining/leaving procedures?

5.3 What are the SA4 plans on post delivery procedures (e.g. point to point repair service)?

5.4 What is the status of HTTP usage for MBMS?

5.5 Other questions

6 Questions from SA4 to SA3

7 Further discussion on technical issues

7.1 Protection of streaming data

Tdoc 17 (LS from SA3 to SA4) was opened for discussion. SA3 asked for some further clarification on the use of SRTP. The SA4 delegates clarified that SRTP is used for the integrity protection of PSS and is optional to implement at the UE. The reason for this choice was driven by the requirements of OMA DRM. SA3 also asked about the other methods that were hinted at by SA4 in their response. It was verbally reported that the RTP wrapper payload for OMA DRM was a possible solution, but no technical proposal was received at this joint meeting. The SA4 delegates in the meeting stated that SA4 are happy with SRTP as a technical solution. The joint meeting agreed that the Editor's note on SRTP in the SA3 specification could be deleted before the specification was presented to the September SA plenary for approval, subject to e-mail approval on the SA3 list.

Tdoc 2 (Ericsson) describes the overlap between the SA3 and SA4 work on MBMS security and in particularly how the combination of MIKEY and SRTP could be used. Much of the document had been covered by earlier discussions (see **tdocs 12**, **13**, **14**, **15** and **17**). The document emphasized that DRM and MBMS security provided different use cases. The document highlighted four areas of overlap: PTP repair service, streaming protection, download protection and application level joining (if defined by SA4). It was commented that the protection of the PTP repair should really be more general and cover all post delivery functions. It also seems to be the case that there will need to be some application level procedure to initiate the key management and the open questions is how/where to specify this.

There exact combination of integrity and confidentiality protection was discussed. It is noted in clause 5.3 of TS 33.246 that protection is either confidentiality or confidentiality and integrity protection. This seems to be out of line with the requirements and also the desire to have no protection. It was agreed that the clause should be reviewed by SA3.

Tdoc 6 (Samsung) notes that the definition of MKI in clause 6.6.2.1 is incorrect and should also include Network ID and Key Group ID. The meeting agreed that the change was technically correct and should be made to the specification before the presentation to the SA plenary, subject to no objections on the SA3 list. It was also felt that it may be possible to reduce the length of the MKI by knowing some of the parameters implicitly. These ways will be explored for the next two SA3 meetings.

Tdoc 10 (Siemens) proposes a specific order for the protection of streaming data and the application of FEC to the data. It proposes that FEC can and should be applied to the data before it is encrypted i.e. to use default order that is proposed by the RFC3711 (SRTP). There were concerns raised that any architecture should not tie different media types together, i.e. it should be possible to apply different coding overheads to different media streams. It was noted that FEC-encrypt order for streaming might be different to the ordering for download. It was discussed whether the security was weakened by applying FEC first before of encryption, as there would be linear relation in the encrypted data. Ericsson noted that due to the use of salting keys within SRTP encryption they did see no security risk.

The meeting had no problems with the proposed ordering of FEC and encryption for streaming, i.e. apply FEC before encryption. The meeting felt that the SA4 specification was the correct place to capture this ordering. If companies have any security concerns with this decision, they are invited to raise them by bringing in a contribution at the October SA3 meeting so the concerns can be forwarded to SA4.

7.2 Protection of download data

Tdoc 8 (Nokia) proposes the use of OMA Downloadv1 for use in downloading files in MBMS. The process involves pre-processing, e.g. to ensure sufficient resources are available and post-processing, e.g. download complete notification. It is proposed at a minimum that this should at not least be excluded for MBMS. The proposal was considered not mature at this stage for SA3 delegates to comment upon. It was left to SA4 to discuss the acceptance of the proposal in their meetings.

Tdoc 7 (Nokia) proposes to re-use the Discrete Content Format from OMA DRMv2, as the method of confidentiality protecting MBMS downloads. Integrity protection could be added on top of this by using XML signatures. There is some work to be done on how to specify the data is protected by MBMS methods as opposed by DRM techniques. It was questioned whether this proposal would need to be discussed in OMA, as there was concern that it might require changes to OMA specification. The support of a DRM Agent would be optional, as it would only be necessary to support the DCF content format for MBMS. With the DCF format it is possible to include more than one piece of protected content.

Tdoc 3 (Ericsson) proposes the use of XML encryption and XML signatures for the protection of download data in MBMS. The use of S/MIME was ruled out, as there is no standardised way to use shared keys for integrity protection. It was commented that perhaps S/MIME with a MAC might be easier to support, but no conclusion was reached.

Tdocs 7 and **3** were noted, as this decision needs to be taken in SA3. It was felt that a comparison between the two methods would be useful to help SA3 make a decision.

Tdoc 4 (Ericsson) discusses the issue of protection of ptp repair service. It proposes that protection of the repair service can be achieved by using HTTP Digest for authentication and the protection that is already applied to the file i.e. the integrity and confidentiality protection that is already applied to the retrieved file repair blocks. It was noted that HTTP Digest could be used for mutual authentication between the UE and the file repair server.

There was some discussion on whether the MIKEY packet carrying MTK could be downloaded using the repair service or included as part of the actual downloaded file. This would overcome the cases when the MIKEY packet was lost or corrupted. An alternative method would be for the UE to directly request the MTK.

7.3 Key management issues

7.3 Other issues

Tdoc 9 (Siemens) concludes that the delivery confirmation procedure as it is currently described by the SA4 specification is **not** sufficient for reliable charging. Information that is essential to consuming the data should be included (i.e. The MTK). There was general agreement that it is up to SA4 to agree on the appropriate text for inclusion into the SA4 TS which could be based on the proposal of Tdoc 9.

Tdoc 5 (Bamboo) also discusses weaknesses in using delivery confirmation for charging. It proposes the possibility of using a request for a key, as a way of knowing the download was complete. There was some concern about keeping a clear definition of what is wanted in a delivery confirmation. It is up to SA4 to clarify the goal of each of the post-delivery functions clearly (e.g. delivery notification, key delivery, file repair functions). Combined execution of post-delivery functions within one http session should be investigated.

8 Any other business

9 Close of the Meeting (Tuesday, 24 August, 16:00)

10 List of Participants

Name	Company	E-mail
Adrian Escott	**3**	adrian.escott@three.co.uk
Dimitris Vasilaras	Lucent Technologies	dvasilaras@lucent.com
Karl Norrman	Ericsson	karl.norrman@ericsson.com
Marc Blommaert	Siemens	marc.blommaert@siemens.com
Meir Fuchs	Bamboo Mediacasting	meir@bamboomc.com
Michael Roberts	NEC	michael.roberts@nectech.fr
Mireille Pauliac	Gemplus	mireille.pauliac@gemplus.com
Sami Pippuri	Nokia	sami.pippuri@nokia.com
Thorsten Lohmar	Ericsson	thorsten.lohmar@ericsson.com
Tiina Koskinen	Nokia	tiina.s.koskinen@nokia.com
Vesa Lehtovirta	Ericsson	vesa.lehtovirta@ericsson.com
Yanmin Zhu	Samsung	yanmin.zhu@samsung.com