3GPP TSG SA WG3 Security — SA3#37 **S3-050075**
February 21-25, 2005 Sophia Antipolis, France

Source: Siemens

Title: Comments to TS 26.346 V150

Agenda item: MBMS

Document for: Discussion/Decision

1 Introduction and proposed actions for SA3

By means of the LS S3-050008 (S4-040760), SA4 kindly asks SA3 to comment on our present view on security as expressed in the TS 26.346. This paper contributes the Siemens comments on section 4.4 of TS 26.346. These identical comments (section 2 of this contribution) were posted on both SA3 and SA4 mailing list on the 9th of Februar, but no comments were received until just before the SA3#37 document deadline.

Proposed actions for SA3:

1 Discuss the security functions (and appropriate naming) of the BM-SC sub functional structure (Figure 4).

2 Align the SA3/SA4 terminology that is used for MBMS user service application layer joining and leaving i.e. it is proposed to distinguish MBMS User Service registration, MSK Key Request and MBMS User Service deregistration within TS 33.246. This would fit with the envisaged SA4 sub function called '(de)registration function'. This also separates the application layer terminology from the bearer level terminology (I.e. MBMS multicast bearer join/leave).

3 Inform SA4 on the need for a MSK key deregistration procedure.

4 SA3 needs to clarify the relationship between an MBMS User Service registration and key management i.e. An MBMS User Service registration is not needed when the MBMS user service needs no protection. The MBMS User Service registration procedure is equal to the first MSK key request of the UE towards the BM-SC.

2 Commented extract from S4-040859 (TS 26.346 V150)

4.4 Functional Entities to support MBMS User Services

Figure 3 depicts the MBMS network architecture showing MBMS related entities involved in providing MBMS user services.

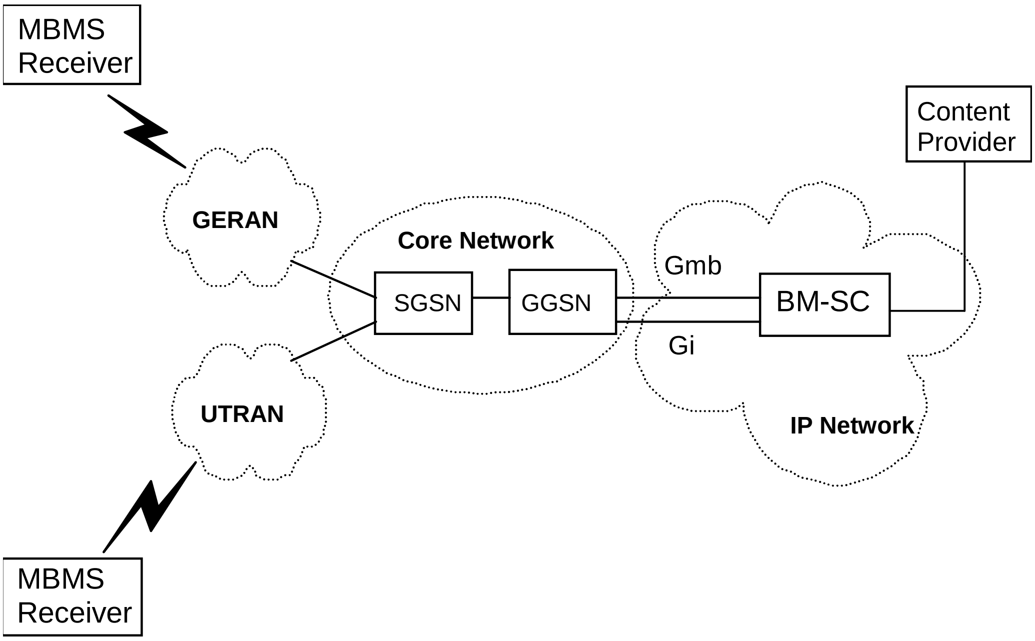

Figure 3: MBMS network architecture model

MBMS User Service architecture is based on an MBMS receiver on the UE side and a BM-SC on the network side.

The use of the Gmb and Gi interface in providing IP multicast traffic and managing MBMS bearer sessions is described in detailed in [4] (TS 23.246).

Details about the BM-SC functional entities are given in figure 4.

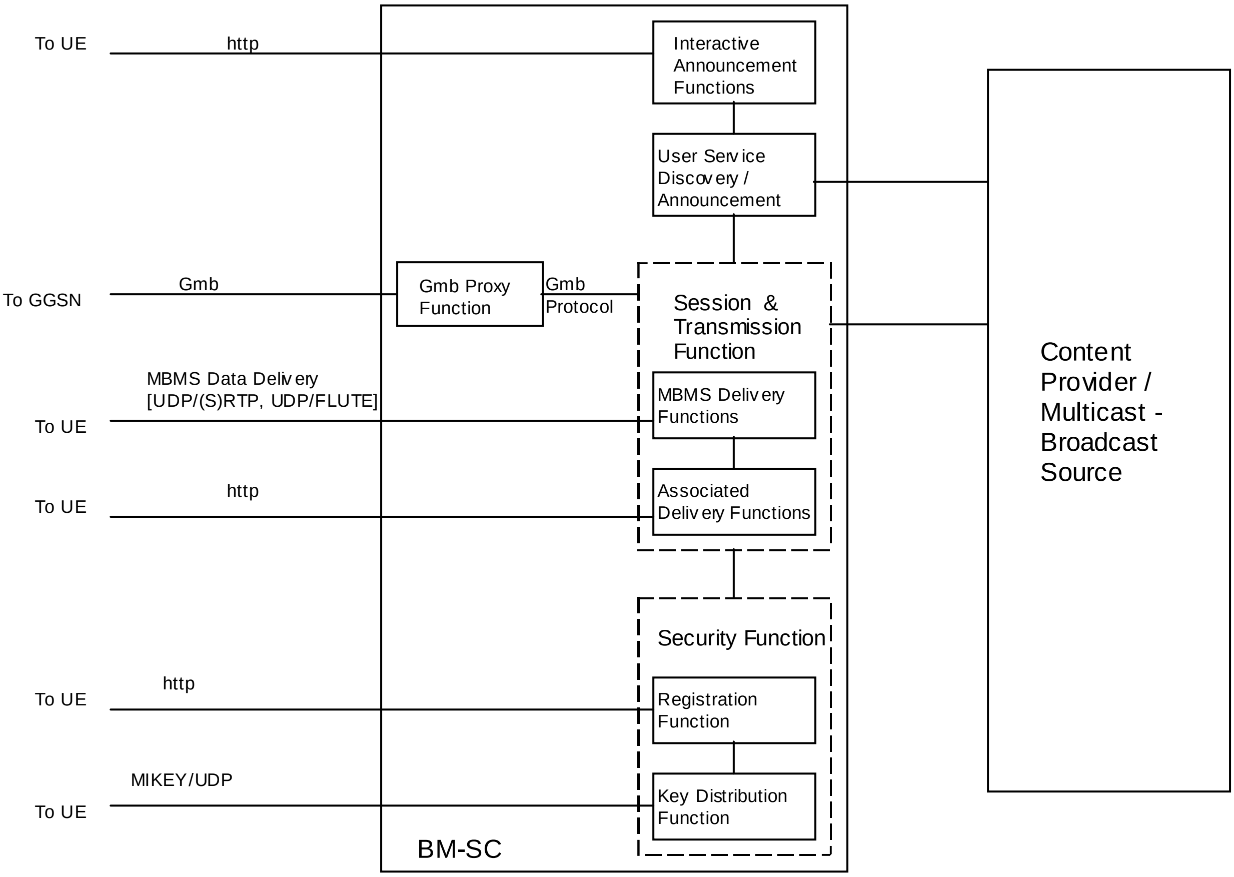
To UE
http
Interactive Announcement Functions
User Service Discovery / Announcement
To GGSN
Gmb
Gmb Proxy Function
Gmb Protocol
Session & Transmission Function
MBMS Data Delivery [UDP/(S)RTP, UDP/FLUTE]
To UE
MBMS Delivery Functions
To UE
http
Associated Delivery Functions
Security Function
To UE
http
Registration Function
MIKEY/UDP
To UE
Key Distribution Function
BM-SC
Content Provider / Multicast - Broadcast Source

Figure 4: BM-SC sub-functional structure

Proposal to change the above figure (I unfortunately have no visio tool : the reasoning behind these proposed changes are given later in the text):

1. rename Security function to 'Key Management' function
2. remove Gmb from inside BM-SC.
3. remove http towards interactive announcement function.
4. add a session protection function before 'session & Transmission' function.
5. registration/deregistration function.

→ SA3: relationship of first key request and 'Registration Function' is to be clarified (see later).

[Editor's note: The http interaction between the MBMS UE and the User Service Discovery / Announcement function in is outside the scope of this specification] If this will not be standardized then it would be better to remove the word http from both the figure and the editor's Note. And if the interface to the user Service Discovery/Announcement is not to be standardized, then how to describe 'standardized security' for it ?

[Editor's note: note that this picture highlights those BM-SC functional elements which are relevant for the SA4 work. For instance, the Security Function depicted here is part of the more general Membership function found in Fig. 5a of TS 23.246. Similar, the User Service Discovery/Announcement and Interactive Announcement functions are part of the more general Service Announcement function found in Fig. 5a of TS 23.246. Better consistency with Fig. 5a of TS 23.246 will be achieved during the final cleanup of this specification]

The Gmb-Proxy function relays the Gmb protocol between the 'Session and Transmission' function and the GGSN.

[Editor's note: SA2 is currently discussing the Gmb Proxy in the architecture. It is currently unclear whether the Gmb Proxy should be a BM-SC sub-function or belongs to an entity between a GGSN and a number of BM-SC functions. It is also unclear whether the Gmb Proxy would be an optional functionality]

The Session and Transmission function is further subdivided into the MBMS Delivery functions and the Associated Delivery functions.

The BM-SC and UE may exchange service and content related information either over point-to-point bearers ~~and~~ or MBMS bearers whichever is suitable. To that end the following MBMS procedures are provided:

- User Service Discovery / Announcement providing service description material to be presented to the end-user as well as application parameters used in providing service content to the end-user

- MBMS-based delivery of data/content (optionally confidentiality and/or integrity protected) from the BM-SC to the UE over IP multicast.

- Key Request and Registration procedure for receiving keys and key updates.

- Key distribution procedures whereby the BM-SC distributes key material required to access service data and delivered content.

- Associated Delivery functions are invoked by the UE in relation to the MBMS data transmission. The following associated delivery functions are available:

    - Point-to-point repair for download delivery method used to complement missing data using point-to-point sessions.

    - Delivery verification and reception statistics collection procedures

The interfaces between internal BM-SC functions are outside the scope of this specification. (why the figure then includes the name Gmb-protocol inside of the BM-SC ?)

4.4.1 Content Provider / Multicast Broadcast Source

The Content Provider/Multicast Broadcast Source may provide discrete and continuous media, as well as service descriptions and control data, to the BM-SC to offer services via MBMS broadcast- and multicast bearer services at a time. An MBMS User Service may use one or several MBMS delivery methods simultaneously. The Content Provider/Multicast Broadcast Source may also be a 3rd Party Content Provider/Multicast Broadcast Source.

The Content Provider/Multicast Broadcast Source function may reside within the operator's network or may be provided from outside the operator's network. The Content Provider/Multicast Broadcast Source can also configure the Session and Transmission functions (e.g. delivery or associated delivery). The interface between the Content Provider/Multicast Broadcast Source and the BM-SC is outside the scope of this specification.

4.4.2 MBMS Security Function

MBMS user services may use Session protection ~~security~~ functions for integrity and/or confidentiality protection of MBMS data. The MBMS key management ~~security~~ function is used for distributing MBMS keys ~~(Key Distribution Function)~~ to authorized UEs. UEs request the (initial) keys from the BM-SC. A first http key request will ~~and register (using the Registration Function)~~register the UE to receive further key updates by key management procedures. If the MBMS users service does not require session protection, then the UE does not need to request keys (i,e. register)

Detailed description of the security functions is provided in [20] (TS 33.246).

[Editor’s Note: The MBMS Security function is to be confirmed by SA3]

SA3 has to study the need for a deregistration function in order avoid needless MIKEY PUSH messages.

4.4.3 MBMS Session and Transmission Function

The MBMS Session and Transmission function transfers the actual MBMS session data to the group of MBMS UEs. The MBMS Session and Transmission function interacts with the GGSN through the Gmb Proxy function to activate and release the MBMS transmission resources.

The function contains the MBMS delivery methods, which use the MBMS bearer service for distribution of content. Further this function contains a set of Associated-Delivery Functions, which may be invoked by the UE in relation to the MBMS data transmission (e.g. after the MBMS data transmission).

The BM-SC Session and Transmission function is further described in later clauses of this specification as well as in [4] (TS 23.246).

If MBMS session protection is ~~security functions are~~ activated for the MBMS User Service, the confidentiality and/or integrity protection is applied by the BM-SC to outgoing MBMS data transmissions. The MBMS session ~~traffic~~ protection is applied between the BM-SC and the UEs. The MBMS session ~~security~~ protection is based on symmetric keys, which are shared between the BM-SC and the UEs accessing the service. For further details on MBMS session ~~traffic~~ protection see [20] (TS 33.246).

[Editor’s Note: The MBMS Security function is to be confirmed by SA3].

4.4.4 Gmb Proxy function

The Gmb Proxy function relays the Gmb protocol and may fill in the MBMS bearer service oriented attributes. The BM-SC Proxy function is described in [4] (TS 23.246).

[Editor’s note: SA2 is currently discussing the Gmb Proxy in the architecture. It is currently unclear whether the Gmb Proxy should be a BM-SC sub-function or belongs to an entity between a GGSN and a number of BM-SC functions. It is also unclear whether the Gmb-Proxy would be a mandatory functionality]

4.4.5 User Service Discovery / Announcement function

The User Service Discovery / Announcement provides service description information, which may be delivered via an MBMS bearer or via the interactive announcement function.

[Editor’s note: Description of the User Service Description / Announcement function in this clause is ffs]

[Editor’s note: The http interaction between the MBMS UE and the User Service Discovery / Announcement function in   is outside the scope of this specification] what is meant here ? that it will not be standardized ? Then it would be better to remove the word http from both the figure and the editor’s Note.

Note: even if it is specified that the announcement may be delivered over MBMS bearer then it would still apply that the protocol would not be standardized, hence leaving the task open for 3GPP SA3 to secure the function.

4.4.6 Interactive Announcement Function.

An Interactive Announcement Function may offer an alternative means to provide service descriptions to the UE, e.g. using HTTP. The specification of this function is out of scope of this document.

4.4.7 MBMS UE

The MBMS UE hosts the MBMS User Services receiver function. The MBMS receiver function may receive data from several MBMS User Services simultaneously. According to the MBMS UE capabilities, some MBMS UEs may be able to receive data, belonging to one MBMS User Service from several MBMS Bearer Services simultaneously. The MBMS receiver function uses interactive bearers for user service initiation / termination, user service discovery and associated delivery procedures.

In case the MBMS user service is secured, the UE needs one or more cryptographic MBMS service keys, therefore the UE requests the relevant cryptographic MBMS service keys using the MBMS registration ~~security~~ function by requesting keys~~s~~. The received keys are then used for securing the MBMS ~~current~~ session related to the received MSK.

[Editor's Note: The MBMS Security function is to be confirmed by SA3].