3GPP TSG SA WG3 Security — S3#25 **S3-020505**

8 - 11 October 2002

Munich, Germany

Source: **Siemens**

Title: **MBMS security functions**

Document for: **Discussion**

Agenda Item: **7.19**

Abstract

This contribution describes the needed security functions for MBMS and analyses the allocation of these security functions to the NE's from the viewpoint of security re-usability.

1) Introduction

The following three main areas for security are identified for the multicast service of MBMS (See figure 1 [TR 23.846 V1.2.0] for the MBMS architecture) :

Function 1: User authentication/authorisation for registration messages to join or leave a multicast group.

Function 2: Encryption of MBMS data to prevent unauthorised reception of multicast data.

Function 3: Content provider authentication/authorisation and integrity protection of content data delivery to the service centre.

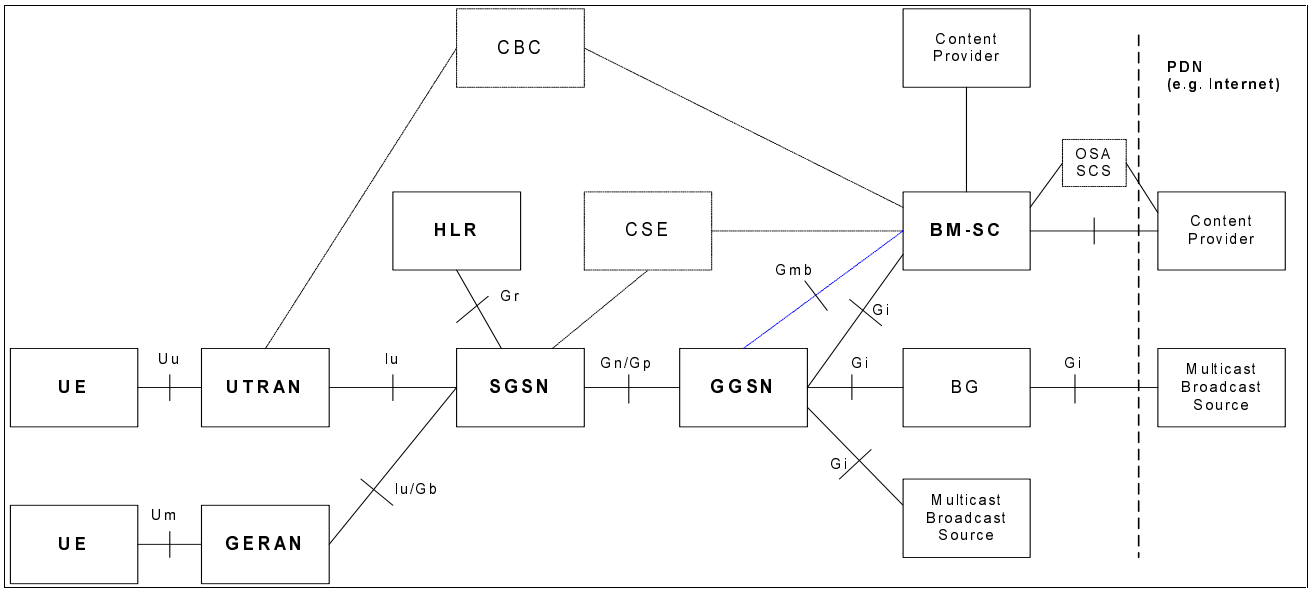

Figure 1: MBMS architecture

The architectural guideline 4 in [TR 23.846 V1.2.0] describes :

" MBMS architecture should re-use, to the extent possible, existing 3GPP network components and protocol elements thus minimizing necessary changes to existing infrastructure and providing a solution based on well-known concepts."

The further paragraphs in this contribution analyse the allocation of the needed MBMS security functions with special attention to the above reuse-principle.

2) User authentication/authorisation for registration messages to join or leave a multicast group.

Function 1 is needed to ensure that no unauthorised users join a multicast group, and that nobody can de-register somebody else from a multicast group. Authentication and authorisation functions have been allocated to the SGSN for both UMTS and GSM packet switched services. This therefor seems to be the obvious way for reusing security functionality. The authorization of registration messages to join or leave a multicast group may rely on the PS domain authentication which is performed in the SGSN. This leaves out the need for an additional authentication mechanism.

Some architectural options in [TR 23.846 V1.2.0] however may allocate Function 1 on the BM-SC. However, new application layer authentication functions would be required in the UE and the BM-SC. In addition, the UE and the BM-SC do not share a key, and it is not obvious how they could obtain a shared key for authentication.

Conclusion: The use of existing authentication and authorisation functions in the SGSN is preferred. The allocation of such functionality at application layer in the UE and the BM-SC would reinvent this functionality and requires more effort.

3) Encryption of MBMS data to prevent unauthorised reception of multicast data.

Function 2 is needed to ensure that no unauthorised users can use the MBMS information multicast on the air if they did not join the MBMS service. Integrity protection is not needed for this purpose. The main questions here are:

1) Where should encryption be performed?

2) Which network element should generate the MBMS keys and how can MBMS[1] keys be obtained by the UE and the encrypting entity in the network (key generation and distribution problem).

1) The re-use of existing 3GPP security functionality would speak in favour of encryption between RNC and UE using the same mechanisms as for ptp connections. But the feasibility of this approach requires more information on the details of the MBMS realisation (More below). If the encryption of multicast data would be done by the BM-SC then an encryption mechanism at the application layer would be needed. This requires that the UE and the BM-SC can generate the necessary security association based on either shared secret information or asymmetric key techniques.

2) The MBMS keys can be randomly generated by the appropriate network entity. They need to be distributed to the UE over encrypted ptp channels. The encryption keys for the MBMS key distribution ptp channels need to be provided as well. The re-use of existing 3GPP security functionality speaks in favour of solutions where encrypted ptp channels are already available. This is the case for SGSN-UE (Gb) or RNC-UE (Iu). In both cases, the MBMS key generation could be done in the SGSN. In the Iu case, RANAP procedures could be used to distribute the MBMS keys from the SGSN to the RNC. Routing area update and/or service control messages could be used to distribute the MBMS key to the user. Key distribution done by the BM-SC at application layer, necessitates application layer mechanisms for authentication of the UE and a confidentiality protection mechanism of the MBMS key transfer to the UE. When key changes would be very frequent then this will result in a high signalling load for the BM-SC.

[1] MBMS key : An encryption key shared by the multicast source in the network (to be defined) and the UE's that joined a multicast group. Its function is to prevent unauthorised UE's from consuming multicast data.

Conclusion: Application layer[2] based MBMS key distribution by the BM-SC has the disadvantage of requiring additional authentication and confidentiality mechanism whereas other signalling layer based key distribution may reuse existing security functions of the core and radio network.

4) Content provider authentication/authorisation and integrity protection of content data delivery to the service centre.

This function is necessary to ensure that no unauthorised content provider can send content to multicast or broadcast users. This may also be required for content provider charging purposes. There is however no need to standardise this function as this interface (See Figure 1) is outside the responsibility of 3GPP.

5) Conclusion

It is preferred to allocate the MBMS security functions 1 and 2 not to the BM-SC at the application layer as it would give rise to additional authentication/encryption functionality and complexity.

For security function 3 , the SA2 view can be confirmed that there is no need for standardization (See [TR 23.846 V1.2.0] clause 7.1.8)

Siemens proposes to inform SA2 of the above conclusions such that the selection of the architectural options can proceed.

6) References

[TR 23.846 V1.2.0]: 3GPP TR 23.846 V1.2.0 MBMS Architecture and Functional Description. Version presented to SA#17,Sept 2002, France.

[2] Application based distribution runs in the PS domain user plane in contrast with signalling based MBMS key distribution.