3GPP TSG SA WG3 #29 **S3-030393**

15-18 July 2003

San Francisco, USA

Agenda Item:	7.20 MBMS
Source:	Alcatel
Title:	Authentication in MBMS
Document for:	Discussion and decision

1. Scope

This paper proposes to use the generic bootstrapping application security mechanism specified in [1] for authentication between the UE and the BM-SC for MBMS. With this bootstrapping mechanism authentication between UE and BM-SC is based on AKA as was also defended in previous contributions. It has however the advantage that there is no need for a new direct interface between the BM-SC and the HSS which is particularly useful when the BM-SC does not belong to the home PLMN. Additionally it removes the problems related to the use of the sequence number matrix from the MBMS work item.

2. Introduction

At SA3 #27 and #28 it was decided that encryption for MBMS traffic shall take place between the BM-SC and the UE and that the BM-SC shall be responsible for traffic encryption key (TEK) generation and disctribution to the UE. Encryption for MBMS traffic in the BM-SC is optional. It was left ffs whether for services as DRM, when encryption of the content is already provided outside the BM-SC, the operator should be able to switch off encryption in the BM-SC.

This document proposes a mechanism for authentication between UE and BM-SC in MBMS. This mechanism is in line with the previously made assumption (e.g. in Ericsson paper S3-030248) that authentication will be based on AKA.

3. Discussions

3.1 Boostrapping architecture

Figure 1 illustrates the general bootstrapping architecture as defined in [1]. The goal of this general bootstrapping architecture is to have one new network element, called the Bootstrapping Server Function (BSF), that has an interface to the HSS and that runs AKA with UEs (described as protocol A) to bootstrap application security between that UE and a priori any application server. In the context of MBMS using this general bootstrapping mechanism avoids that the BM-SC needs to interface with the HSS.

After running protocol A, the UE and network (BSF) are mutually authenticated and share secret key material Ks = CK||IK. Additionally the BSF provides the UE with a unique identifier which can be used to identify UE and Ks e.g. to a Network Application Function (NAF).

After running protocol A the UE authenticates to the NAF using Ks via the B reference point. This protocol depends on the specific application and we make a proposal for protocol B for MBMS in the next section.

The D reference point unables the NAF to fetch the key material Ks for a particular UE. It may also be used to fetch subscriber profile information.

Protocol C is used between the BSF and the HSS. It is used by the BSF to fetch AVs and profile information for a specific user. Protocols A, C and D are appplication-independent and are being specified in [1].

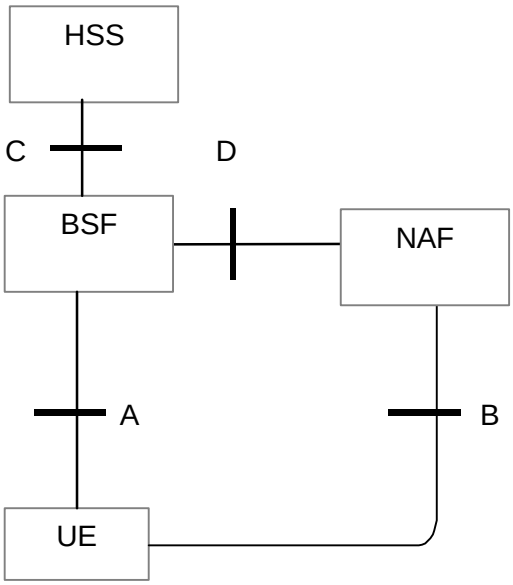

Figure 1 Simple network model for bootstrapping

3.2 Use of bootstrapping architecture for UE - BM-SC authentication

In the context of MBMS the BM-SC takes up the role of the NAF. Rather then running AKA directly with the BM-SC, the UE runs AKA with the BSF, protocol A in Figure 2. This mechanism has the advantage that the BM-SC does not need to have a direct interface with the HSS. This is in any case a plus but is particularly desirable in the case where the BM-SC does not reside in the home PLMN.

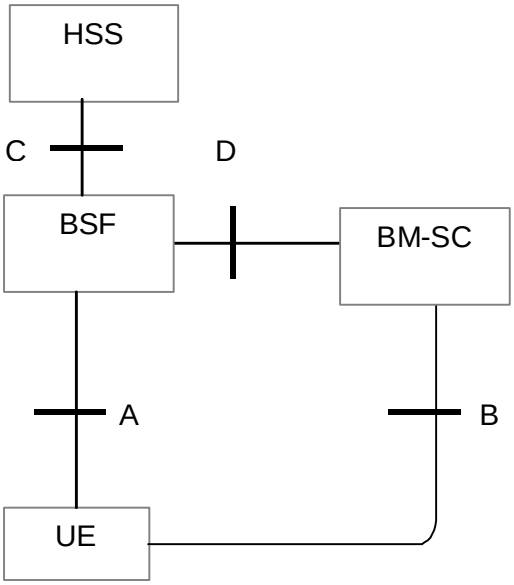

Figure 2 Simple network model in MBMS architecture

Subsequently the UE contacts the BM-SC to request a specific MBMS service. If the BM-SC decides that authentication is required it replies with an authentication request containing a challenge. The UE replies with an authentication message that uses the challenge and IK (or a key derived from IK) as input. The UE also includes the identifier it received from the BSF in his response to the BM-SC.

If the BM-SC has no shared secret that corresponds to that UE and to that Identifier then it contacts the BSF over the D interface. The protocol that shall run over the D interface is currently being defined under the work item Support for Subscriber Certifictaes, see [1]. Note that IK is part of the key material Ks = CK||IK.

The BM-SC checks the authentication message of the UE and if authentication is succesful, the BM-SC sends the required TEK to the UE. The cipher key CK which is part of Ks and is hence shared between the UE and the BM-SC or a key derived from CK can be used to encrypt the TEK for transport from the BM-SC to the UE. Key derivation, if required is ffs. Transport of the TEK can be done using Mikey (see [2]) as was proposed by Ericsson in previous contributions.

Note that it would be possible that the UE initiates a connection with the BM-SC and only after receiving an unauthorized message decides to run protocol A. After this run of protocol A the UE re-contacts the BM-SC as described above.

3.3 Proposal for protocol B between the UE and the BM-SC

Authentication of the UE towards the BM-SC could be done using HTTP Digest.

1. UE -> BM-SC: HTTP request identifying the UE and the MBMS group the UE wants to subscribe to.
2. BM-SC -> UE:*401 unauthorized* message including a www-authenticate header containing a nonce to be used in the HTTP Digest protocol.
3. UE -> BM-SC: authorization header containing a message digest computed over the previously received nonce (and some other data) with IK or a key derived from IK as shared secret.
4. BM-SC -> UE: authentication-info header to indicate success of authentication + Mikey message containing the TEK, encrypted with CK or a key derived from CK. The latter of course only if the requested MBMS service is confidentiality protected. The BM-SC may use IK or a key derived from IK to authenticate and integrity protect this message.

The use of HTTP Digest is only one possibility and other alternatives could also be considered.

4. Conclusions

It is proposed that the generic application security bootstrapping mechanism that is being defined in the context of support for subscriber certificates in [1], is used for authentication between UE and BM-SC in the context of MBMS. This bootstrapping mechanism is agreed to be a generic mechanism that generates shared secret key material that can subsequently be used to bootstrap application security.

Advantages of this approach include

- No need for a new direct interface between the BM-SC and the HSS. Limiting the number of Network Elements that interface with the HSS is in any case good but it is particularly beneficial when the BM-SC is not part of the HPLMN.
- Issues related to sequence number space and anti-replay mechanism only need to be addressed once rather than for each and every new application separately.

5. References

[1] S3-030203 draft TS ab.cde Bootstrapping of Application Security using AKA and Support for Subscriber Certificates, (Release 6), version 0.2.0.

[2] Mikey: Multimedia Internet KEYing, draft-ietf-msec-mikey-07.txt, June 2003.

[3] 3GPP TS 23.234, Technical Specification Group Services and System Aspects; Multimedia Broadcast/Multicast Service (MBMS); Architecture and Functional Description (Release 6), version 0.4.0.

[4] 3GPP TS 33.246, Technical Specification Group Services and System Aspects; Security; Security of Multimedia Broadcast/Multicast Service (Release 6), version 0.0.4.