3GPP TSG SA WG3 #28 **S3-030248**

6-9 May 2003

Berlin, Germany

Agenda Item: 6.21 MBMS

Source: Ericsson

Title: Authentication in MBMS

Document for: Discussion and decision

1. Scope

This paper aims to discuss different proposal on how the authentication framework can be implemented in the MBMS architecture; and proposes as a conclusion that a new authentication procedure based on AKA is supported between the BM-SC and the UE for MBMS. Ericsson sees Digest AKA as the preferred protocol.

It shall also be noted in this contribution that Ericsson will not further discuss EAP-AKA as a potential protocol for a new authentication procedure at the application layer between the BM-SC and the UE.

2. Introduction

At SA3 #27 it was decided that encryption for MBMS traffic shall take place between the BM-SC and the UE. Encryption for MBMS traffic in the BM-SC is optional. For other services as DRM, when encryption is already provided of the content outside the BM-SC, the operator should be able to switch off encryption in the BM-SC.

Two other outstanding issues related to security in MBMS are:
1) how the authentication procedure in MBMS shall be supported in the MBMS architecture; and also
2) how the MBMS encryption key distribution shall be supported in MBMS.
These two issues are very related, but only issue 1) is discussed in this paper. For discussion on MBMS encryption key distribution, see contribution [Key generation and distribution] from Ericsson.

It is assumed in this paper that authentication is based on AKA and not on other security mechanisms as e.g. certificates. In addition the scenario with multicasting DRM content via the MBMS architecture, will be discussed as well.

Terminology used in this paper:

TEK – the common encryption key, encrypting the MBMS data broadcasted to all users.

CK – the pre-shared encryption key in the UE and the network node (e.g. SGSN or BM-SC) is, a) used by the network to encrypt the TEK before distributing the TEK to the UE; and b) used by the UE to decrypt the TEK. CK is delivered by the USIM to the UE and shared with the network at AKA.

3. Discussions

Two main alternatives that are discussed in this paper for authentication in MBMS are:

1. Re-use of UMTS AKA between the SGSN and the UE; and
2. A new authentication procedure for AKA between the BM-SC and the UE.

A third option was presented in the SA2 #30 meeting from Siemens in contribution S2-030641, where it was proposed to re-use the IMS AKA in the IMS architecture for MBMS. This proposal requires an IMS network in the 3GPP operators network and therefore this should be seen as an optional architecture in order to support MBMS and provide AKA in MBMS. This third option will not be further discussed in this paper.

3.1 Purpose of AKA for authentication in MBMS

Introducing authentication based on AKA has two means in MBMS:

1. mutual authentication, i.e. user authentication and network authentication;

2. retrieve a shared encryption key, CK, in the UE and the network from AKA, to be used to protect the MBMS encryption key at the key distribution from the network to the UE according to requirement R5a in 33.246.

3.2 Re-use of UMTS AKA between the SGSN and the UE

One solution is to re-use the already existing authentication procedure as UMTS AKA between the SGSN and UE. Then a shared encryption key, CK, is retrieved and stored in the UE and the SGSN.

Notice that the following discussion in this chapter focus on the architecture issues with performing AKA between the SGSN and the UE, and the issues related to the required key handling in the MBMS architecture with this approach.

The TEK (MBMS encryption key) could be transported in two different ways from the network to the UE, see contribution in [Key generation and distribution]:

(1) MBMS encryption key is generated by the BM-SC and also distributed by the BM-SC to the UE at the application layer. Issues and problems can be foreseen in the network and the UE with this approach:

- It needs to be resolved how the shared encryption key, CK, shall be transferred from the SGSN to the BM-SC.

- How can synchronisation problems be avoided, in order to ensure that the BM-SC is always using the currently used and shared CK in the UE and SGSN, to encrypt the TEK (MBMS encryption key)?

- Layering issues in the UE: the CK is generated in one layer (GMM) and required in the application layer in order to decrypt the TEK (MBMS encryption key) distributed to the UE at the application layer.

(2) MBMS encryption key is generated by the BM-SC but distributed by the SGSN to the UE in the GPRS Mobility Management (GMM) protocols. Issues and problems can be foreseen in the network and the UE with this approach:

As the TEK (MBMS encryption key) distribution is performed in the GMM protocols from the SGSN to the UE, the encryption and decryption of the TEK (MBMS encryption key) by using the shared encryption key, CK, can be performed in the same GMM layer in the SGSN and the UE. Still other layering issues remains with the TEK (MBMS encryption key), which are discussed in the Ericsson contribution on “Key distribution in MBMS”.

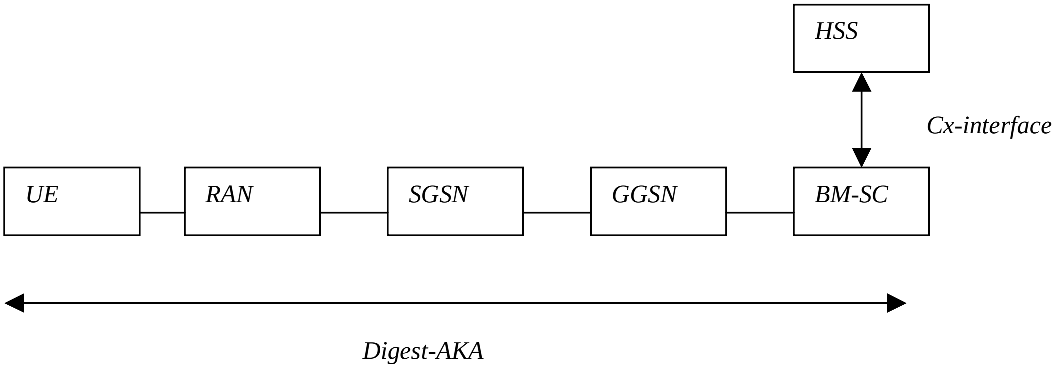
3.3 New authentication procedure between the BM-SC and the UE

A second solution could be to introduce a new authentication procedure between the BM-SC and the UE using HTTP Digest AKA. It seems that a variant of the “interleaving attack” described in [S3-030069] also applies for this solution. In MBMS context, the attacker is not able to interpret the encrypted MBMS data, however, the attacker may be able to subscribe to the services and initiate charging records on behalf of the victim. For this reason, the “interleaving attack” should be mitigated also in MBMS context if HTTP Digest AKA is applied. One approach to solve the problem is to use the HTTP Digest AKAv2 [S3-030xxx] instead of AKAv1 [RFC3310].

Another issue is whether MBMS should have a separate sequence number (SQN) space in the network, just as the CS, PS and IMS domains have with the USIM? This should be FFS. See [4] on sequence number management

In order to re-use AKA for MBMS, BM-SC needs to have an interface for HSS. In the IMS architecture, the HSS delegated the responsibility to perform AKA to the S-CSCF. The S-CSCF is always located in the HPLMN. Digest AKA was chosen as the protocol for IMS AKA. Digest AKA terminates in the S-CSCF. The BM-SC in MBMS could take a similar role as the S-CSCF in IMS, where the BM-SC has the responsibility to perform AKA. The Cx-interface in

IMS between the HSS and S-CSCF could then also be re-used in MBMS architecture between the HSS and the BM-SC, when the BM-SC resides in the HPLMN.

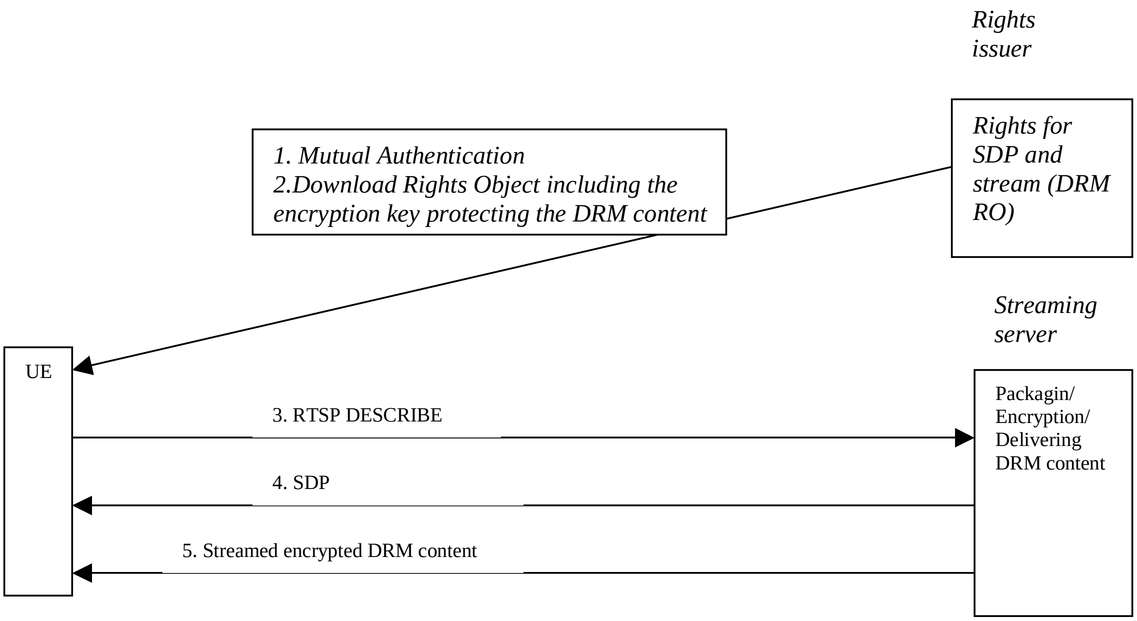


3.4 DRM phase 2 and MBMS

3.4.1 Background on authentication in DRM phase 2 in OMA

In OMA the standardization on DRM phase 2 is currently ongoing and not completed yet.

The mutual authentication in DRM will be based on certificates and is performed already in the phase when Rights Objects are downloaded to the UE. This phase takes place, prior to the phase when downloading DRM content to the UE. Therefore the authentication procedure in DRM has no impact on the MBMS architecture or any impacts on the discussions on the authentication procedure in the MBMS architecture (see figure below).

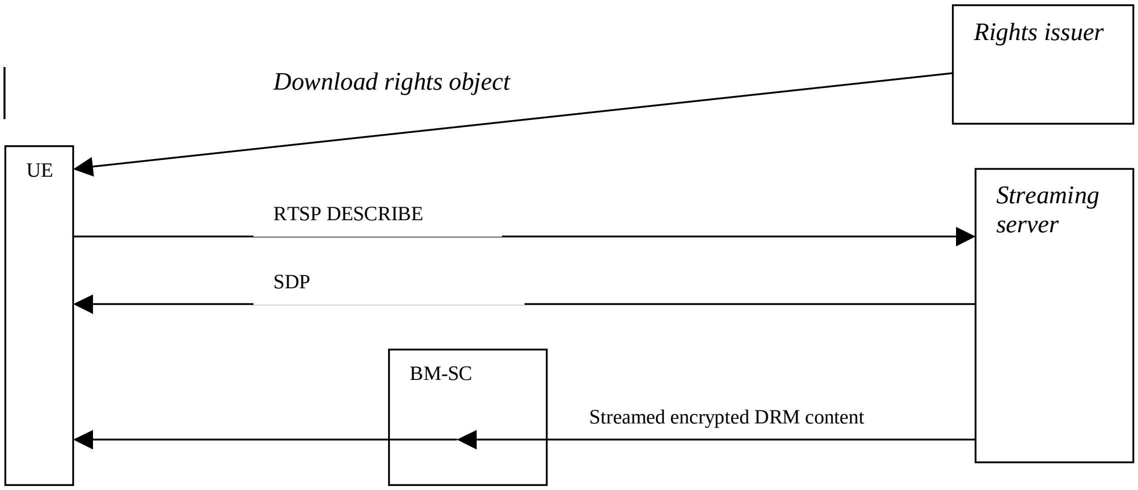


3.4.2 DRM content multicasted via MBMS to the UE

In the case when DRM is multicasted to the UE via the MBMS architecture, the DRM content is already encrypted when reaching the BM-SC. In this case the 3GPP operator could either:
- perform an additional encryption in the BM-SC on the DRM content; or
- switch off encryption in the BM-SC.
This should be a 3GPP operator choice.

In the case when the BM-SC performs encryption on the DRM content, a shared encryption key, CK, is required in the UE and the network (e.g. SGSN or BM-SC) in order to protect the MBMS encryption key at key distribution to the UE. Therefore AKA is required in this case.

In the case when the 3GPP operator has switched off the encryption in the BM-SC for the DRM content, no shared encryption key, CK, is required in the UE and the network (e.g. SGSN or BM-SC). If we go for the solution when the authentication procedure takes place between the BM-SC and the UE, the 3GPP operator could in this case still want to execute the AKA in order to have mutual authentication of the UE and the network (BM-SC), but this could be an operator choice.



4. Conclusions

Re-use of authentication between the SGSN and the UE:

If the authentication procedure UMTS AKA between the SGSN and the UE is re-used, then this solution would make the security framework for MBMS *access dependent*.

No impacts are foreseen on this solution when DRM content is multicasted to the UE, as the execution of UMTS AKA is performed independent of the MBMS architecture and performed regardless of what the type of MBMS traffic that is multicasted.

Issues, as synchronization problems, i.e. how to ensure that the BM-SC is always using the currently used CK in the SGSN and the UE; and also layering issues i.e. how to provide and transfer the security keys between the GMM layers and layers above the IP-stack in the UE, *does not promote a good security solution* in the network and the UE, for MBMS services.

New authentication procedure between the BM-SC and the UE:

There are no layering issues in the network and the UE with this solution. This solution would make the security framework for MBMS *access independent*. Note that SA2 is planning to introduce MBMS via WLAN access in REL-7 or later releases.

When the DRM content is multicasted to the UE via MBMS, does not have any major impact on the MBMS architecture. Initiation of AKA from the BM-SC should be optional and an operator choice, in the case when encryption is switched off in the BM-SC for the DRM content.

The drawback with this solution is that a new authentication procedure between the UE and the BM-SC is required in the MBMS architecture.

5. Proposal

Ericsson proposes to introduce a new authentication procedure based on AKA between the BM-SC and the UE. Ericsson sees Digest AKA as the preferred protocol.

It would be preferred if the authentication framework in the IMS architecture could be followed for the MBMS architecture, where the AKA terminates in the BM-SC and the HSS delegates the responsibility to the BM-SC to decide when to initiate AKA. The Cx-interface could be re-used between the BM-SC and the HSS in MBMS.

In addition, Ericsson proposes to send an LS to SA2 and CN4, asking:

- Whether SA2 agree on the analyze on the relation between DRM and MBMS presented in this paper;
- Whether SA2 agrees upon that the MBMS architecture could follow a s similar approach as in the IMS architecture where 1) the AKA procedure terminates in the BM-SC; and 2) the HSS delegates the responsibility to the BM-SC to decide whether to initiate AKA or not; and
- Whether CN4 sees any problems with using the Cx-interface between the HSS and the BM-SC in the MBMS architecture.

6. References

[1] 3GPP TS 22.146, Technical Specification Group Services and System Aspects; Multimedia Broadcast/Multicast Service;Stage 1 (Release 6), version 6.2.0.

[2] 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.

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

[4] 3GPP TS 33.102, Technical Specification Group Services and System Aspects; Security; Security architecture (Release 5), version 5.1.0.

[Key generation and distribution] S3-030xxx ‘Key generation and distribution in MBMS’, from Ericsson.

[S3-030069] The use of HTTP in Presence/IMS, contribution from Ericsson to SA3#27.

[S3-030xxx] HTTP Security in Mt interface, contribution from Ericsson to SA3#28.