3GPP TSG SA WG3 #26 **S3-020641**

19-22 November 2002

Oxford, UK

Agenda Item: MBMS

Source: Ericsson

Title: Key distribution at Application Layer for MBMS

Document for: Discussion

1. Introduction

This paper discusses the key handling and the key distribution from the BM-SC to the UE for MBMS services at the Application Layer.

Several potential solutions can be used for key management and authentication. Solutions as HTTP or RTSP, Digest AKA and MIKEY are some Ericsson preferred solutions that are discussed in this paper. Other protocols could be considered as well as EAP-AKA.

SA3 should continue the study of the Application Layer Security and make further investigations to the next SA3 meetings on the proposals presented in this paper.

2. Background

In the latest version of TS 33.cde we have the following security requirements discussed at the SA3 #25:

R1a: A valid USIM shall be required to access any 3G service including the MBMS service.

R1b: It shall be possible to prevent intruders from obtaining unauthorized access of MBMS services by masquerading as authorized users.

R2a: It shall be possible for service providers (i.e. BM-SC) to authenticate users at the start of, and during, service delivery to prevent intruders from obtaining unauthorized access to MBMS services.

R2b: It shall be possible to prevent the use of a particular USIM to access MBMS services.

R4a: It shall be possible to protect the confidentiality of MBMS multicast data on the radio interface.

R4b: The MBMS multicast data may be encrypted with a common encryption key, which shall be available to all users that has joined the MBMS service.

R4c: The encryption key(s) and the integrity key for the MBMS multicast service shall be encrypted when delivered to the users. In addition, it may be required to protect these keys with a MAC.

R4d: Only the valid users that has joined a MBMS multicast service shall be able to decrypt the encryption key(s) and the integrity key delivered from the network.

R4e: Mandate support of re-keying in the UE and BM-SC in order to ensure that users that has joined a MBMS service, but then left, shall not gain MBMS multicast service without being charged.

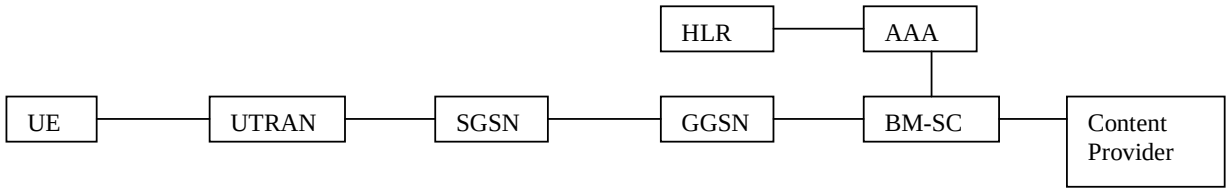
This paper attempts to discuss some proposals on how to fulfill these requirements.

The approach of Security Protocol at Application Layer is promoted in this contribution for several reasons as:
a) The trust model is between the Home Network, the Content Provider and UE/Subscriber;

b) access independent i.e. it can be used over GERAN, UTRAN and WLAN.
c) Security Protocol as SRTP provides a number of advantages as SRTP is secure for unicast and multicast RTP applications, gives high throughput and low packet extensions and so on…

4. Architecture

The flows discussed in this paper are based on an architecture where a potentially new node is introduced, the AAA node. The AAA node is connected to the BM-SC and the HLR. The AAA node could serve as a transparent node or as as EAP server (if EAP-AKA is used). The AAA node is FFS.



Terminology

The following terminology, regarding the encryption key for MBMS, is used in this paper:

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

KEK – the pre-shared encryption key in the UE and the BM-SC is, a) used by the BM-SC to encrypt the TEK before distributing the TEK to the UE; and b) used by the UE to decrypt the TEK from the BM-SC. The KEK is derived from the CK in the UE and BM-SC. CK is delivered by the USIM to the UE and shared with the BM-SC at AKA. The key derivation functions to produce the KEK are FFS.

5. Discussion regarding key distribution at joining phase in MBMS

5.1 General

The MBMS data, broadcasted to the UE's, is encrypted with a common TEK. The TEK has to be distributed to all the UE's that joins a MBMS service, in order for the UE's to be able to decrypt the MBMS data sent from the BM-SC.

The phase of when the user joins a MBMS service takes place over a PDP context. The initial key distribution of the TEK is performed during the joining phase in MBMS, point-to-point.

If the TEK is changed in the BM-SC after the initial TEK distribution at the joining phase, then this should be done using the re-key function discussed in chapter 5.2 in this paper.

Notice that integrity key has not been considered in this discussion paper for simplicitly. A pre-shared integrity key can be retrieved from the USIM in the UE at a UMTS AKA procedure. In addition, it's still an open issue in SA3 whether the MBMS data shall be integrity protected.

5.1.2. Protocols for authentication and key management

This chapter discuss the protocols that can be used for authentication and key management. Different alternatives are mentioned in this paper:

Alternative 1 - Digest AKA

For authentication the Digest AKA protocol could be a potential solution, which is based on UMTS AKA.

For the purpose of key management and authentication, HTTP (or RTSP) can be used as transport protocol, HTTP Digest AKA as authentication method and MIKEY as key distribution mechanism. The MIKEY messages carrying the TEK are encrypted by the BM-SC with the KEK. In this case, the AKA generated session key, CK, is used as KEK (possible after some key derivation). The KEK is shared between the BM-SC and the UE, and it can be delivered from the USIM to the UE, and from the AAA server to the BM-SC during the HTTP authentication procedure.

Notice that we don't have to use TLS with HTTP as we have the encrypted MIKEY message. HTTP **can** carry MIKEY, but there is not yet any draft or RFC that specifies exactly how.

Notice also that MIKEY has no client-server request. With MIKEY you can only push down keys to the UE. This could be solved by e.g. client sending an HTTP GET that results in a MIKEY over HTTP response.

Alternative 2 - EAP-AKA

In theory, AKA could be integrated to MBMS via EAP-AKA. However, the use of EAP-AKA is not straightforward in MBMS because EAP needs to be integrated into some underlying protocol. EAP is typically used with PPP [RFC-2284], however, IETF PANA WG is currently trying to integrate EAP into some other underlying protocol. For example, there has been an attempt to integrate EAP into UDP. Unfortunately, it seems that the PANA WG will not deliver protocol RFCs in the near future.

Another approach to integrate EAP to MBMS is through [PIC]. PIC (The Pre-IKE Credential provisioning protocol) is a method to integrate legacy authentication methods, such as AKA, for IKE. It can alos be used without IKE for authentication and key generation. In the case of MBMS, PIC could be used for authentication and CK generation. CK can be used to distribute the TEK to the subscriber, e.g. by using MIKEY. Currently, it seems that PIC might be available earlier as a standard then the protocol from PANA WG. However, PIC requires quite many round-trips, and consequently it may not be appropiate mechanism for MBMS.

PANA is currently working on requirements documents for network access. This means that they temporarily have stopped to produce solution documents until the requirements are set and stable. However, discussions on the PANA mailing list indicates that there eventually will be an RFC on carrying EAP in either IP, ICMP, UDP or TLS.

PANA has an expired draft (draft-engelstad-pana-eap-over-udp-00) on how to carry EAP in transport layer protocols. It is suggested that UDP is used for this purpose, but the draft states that it could be used over e.g. TCP with minor modifications. The draft expired in August 2002. This draft is a re-write of a previous one on carrying EAP in IP.

It is suggested that SA3 shall further study the use of EAP-AKA within MBMS.

5.1.3 Protocols to protect the MBMS data

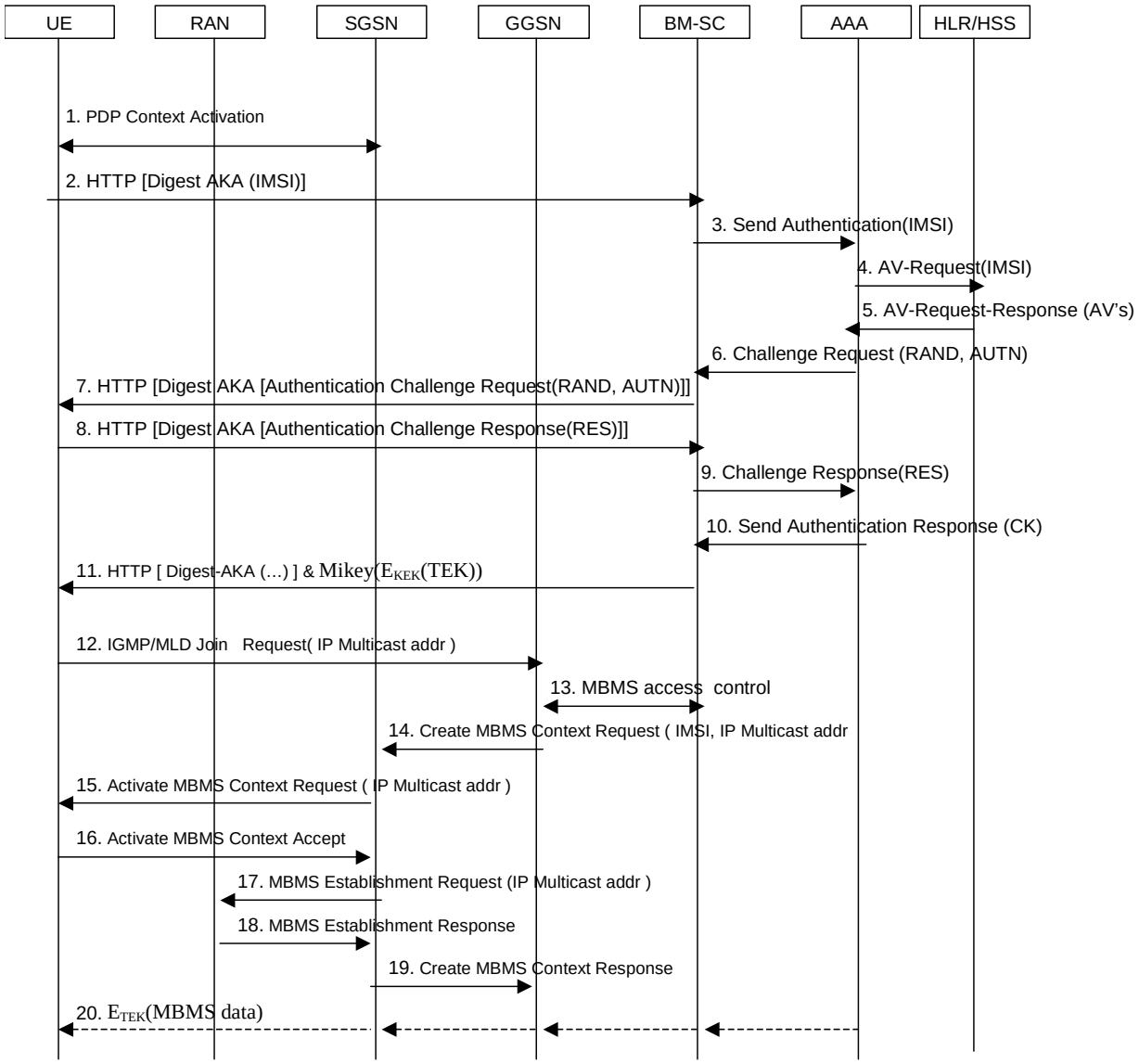
It is assumed that the MBMS data is a RTP packet, which is secured with SRTP. The TEK is used in SRTP to protect the MBMS data. Other protocols than RTP - used to carry the MBMS data, might need to be considered as well, and needs to be FFS.

6. Flows for Alternative 1 - key distribution at joining phase in MBMS

The flow below is based on a Ericsson contribution in S2-023325 presented in SA2 last week. The procedure how to join a MBMS service had not been agreed in SA2 at the point in time when this contribution was written. But to be able to proceed the work in SA3, we had to base this contribution on some assumptions.

This flow is based on Alternative 1 in chapter 5.1.2, using the HTTP protocol. Notice though that RTSP could be used as well.The Digest AKA protocol is carried in HTTP in order to authenticate the UE. The TEK is distributed to the UE in the MIKEY protocol. MIKEY is carried in the HTTP protocol as well.

It is assumed that a PDP context has been established in order to join the MBMS service and that security at the radio access layer is provided, as integrity protection in UTRAN and optionally encryption in GERAN and UTRAN. It also assumed that the UE knows the IP address of the BM-SC in advance.



1.A PDP Context is activated to the APN where the BM-SC is located.

2. The UE sends a request for a specific MBMS service e.g specific by the realm or URL to the BM-SC to authenticate the UE.

3. The BM-SC requests the AAA node to initiate an authentication procedure for a particular subscriber by sending a Send Authentication Request message with the IMSI to the AAA node.

4. The AAA node requests AV's from the HLR/HSS by sending a AV-Request (IMSI) message to the HLR/HSS.

5. Upon receipt of this message, the HLR/HSS responds with a AV-Request-Response message including an ordered array of AV's to the AAA. Each AV contains RAND,XRES, AUTN, CK and IK. The generation of AV's in HLR is performed as specified in TS 33.102. The SQN handling is FFS.

6. The AAA node selects the AV and transmits the RAND and AUTN, that belongs to this AV, to the BM-SC in the Challenge Request (RAND, AUTN) message. Notice that there are several ways to implement that. The Cx interface can be used for this purpose, which would require extensions to the Cx interface.

7. The BM-SC sends the Challenge Request message to the UE in Digest AKA.

8. At reception of this message, the USIM in the UE verifies the AUTN, and if accepted, the USIM computes the signature of the RAND – RES. If the USIM considers the authentication as being successful, the UE returns an Authentication Challenge Response (RES) message to the BM-SC. During generation of authentication vectors, the USIM in the UE also computes a new Ciphering Key (CK), and a new Integrity Key (IK). These keys are stored in the UE.

9. The BM-SC forwards the Challenge Response message to the AAA node.

10. At reception of the message Challenge Response from the BM-SC, the AAA node retrieves the active XRES for that user and uses this to check the response sent by the UE. If the check is successful then the user has been authenticated. The AAA sends a Send Authentication Response (IMSI, Successful, CK, IK) message to the BM-SC node. The BM-SC shall use some derivations functions that are FFS to derive the KEK from the CK.

11. The BM-SC delivers the common TEK, which is encrypted with KEK, to the UE in a MIKEY message (Mikey(E_{KEK}(TEK))).

12. The UE sends a IGMP/MLD Join Request message to the GGSN. The UE uses the established PDP Context to signal what MBMS bearer (IP multicast address) it wants to join. The GGSN shall be IP multicast enabled in order to receive the IGMP/MLD messages. The GGSN fetches the IMSI and MSISDN from the PDP Context on which the join request is received and creates an MBMS UE Context.

13. GGSN executes Access Control procedures towards the BM-SC to verify that the user is authorized to join the service and that the IP multicast address requested by the UE corresponds to a valid MBMS multicast service. IMSI is included in the message to identify the user. The BM-SC authorizes the user, creates an MBMS UE Context and returns an acknowledgement to the GGSN.

14. The SGSN checks in its subscription information that the user has subscribed to MBMS services, and creates an MBMS UE Context, when it receives the Create MBMS Context Request message. The SGSN increments the Number of joined UE's counter in the MBMS Bearer Context. If no MBMS Bearer Context exists, it invokes the MBMS Bearer Context Request procedure to fetch it.

15. The SGSN sends an Activate MBMS Context Request message to the UE to notify that the MBMS context is activated and to link it to the established PDP context.

16. The UE acknowledges the MBMS context activation.

17. The SGSN sends an MBMS Establishment Request to the RAN node. The nature and handling of this message is FFS

18. When RAN acknowledges, the SGSN sends a Create MBMS Context Response to the GGSN.

19. When GGSN receives the response it updates the MBMS UE Context. It is FFS whether the BM-SC needs to be notified on the successful activation or if only failures need to be reported.

20. When the activation is completed and all necessary bearers have been established (see MBMS Bearer Context Request procedure), the MBMS Data encrypted with TEK (E_{TEK}(MBMS Data)) will start to flow if the transmission is ongoing.

7. Discussion regarding re-keying in MBMS

At the re-keying phase the new relevant common TEK, needs to be distributed to all the UE's that has joined a MBMS service.

Re-keying could be done either point-to-point or broadcasted on a common channel to all the UE's.

The MIKEY protocol can be used to distribute the TEK to the UE's. The MIKEY message is encrypted by the BM-SC with a pre-shared KEK. The CK is delivered from the USIM to the UE at UMTS AKA and shared with the BM-SC. The KEK is derived from the CK in the UE and BM-SC by using some derivation functions. Notice though that there is no need to change the pre-shared KEK in order to perform re-keying of the TEK.

If SRTP is used to protect the streaming media, there is a possibility to change the TEK used by two means: either each TEK is associated with a Master Key Identifier (MKI) or each TEK is associated with a lifetime. The lifetime of the TEK is expressed in terms of extended sequence numbers, i.e., the sequence numbers carried by RTP-headers themselves extended locally on sender and receiver side. Both the MKI:s and the lifetimes of the TEK can be exchanged using MIKEY.

It is possible to profile the lifetime of the TEK not only to the sequence number but also to a timer in seconds or hours.

Broadcasted re-keying.

LKH could be a potential solution for broadcasted re-keying. Notice though that there is no support of LKH in MIKEY today. LKH needs to be FFS.

Point-to-point re-keying

Point-to-point re-keying could be performed with a prior optional UMTS AKA procedure.

The possibility for the BM-SC to initiate the UMTS AKA procedure can be useful in the case the BM-SC wants to authenticate the UE to prevent fraudulent users and in the case the BM-SC wants to change the pre-shared KEK in the UE and BM-SC.

It is assumed that a background PDP context is already established at the point of time for re-keying. Note that this background PDP context was established already when joining the MBMS service and is also used to leave the MBMS service.

When the lifetime of the TEK expires in the UE, the UE can initiate a request to the BM-SC in Digest AKA according to message 2 in the flow in chapter 6. When the BM-SC receives the request in Digest AKA, the BM-SC can decide whether it wants to initiate a new UMTS AKA or not. This is an optional decision for the BM-SC.

If the BM-SC decides to authenticate the UE, then an authentication challenge request will be sent to the UE according to message 7 in chapter 6. The USIM verifies the AUTN, and if accepted, the USIM computes the RES, which is forwarded to the BM-SC in an authentication challenge response. A new pre-shared KEK, is delivered from the USIM to the UE as well. The BM-SC has the same pre-shared KEK, which it shall use to protect the MIKEY message containing the new TEK (or old TEK if the BM-SC for some reason does not want to re-key), delivered to the UE in message 11 in chapter 6.

If the BM-SC decides not to authenticate the user, then the BM-SC sends a MIKEY message, which contains a new TEK (or old TEK if the BM-SC for some reason does not want to re-key). This TEK is protected with the old pre-shared key, KEK.

8. Proposal

There are a lot of open issues in SA2 and the RAN groups on MBMS. The join procedure for MBMS has not been agreed yet in SA2, at least not when this contribution is written. The assumptions on the join procedure shown in this paper might be changed.

Several potential solutions can be used for key management and authentication. For the moment the solution with either HTTP or RTSP, Digest AKA and MIKEY is the Ericsson preferred solution. But other protocols could be considered as well as EAP-AKA.

Ericsson proposes that SA3 continues the study of the Application Layer Security and make further investigations to the next SA3 meeting on the proposals presented in this paper, which hopefully can be based on more stable decisions in the other groups as SA2.

9. References

[1] 3GPP TS22.146, Technical Specification Group Services and System Aspects; Multimedia Broadcast/Multicast Service;Stage 1 (Release 6), version 6.0.0.

[2] 3GPP TR 23.846, Technical Specification Group Services and System Aspects; Multimedia Broadcast/Multicast Service; Archietcture and Functional Description (Release 6), version 1.2.0.

[3] Tdoc S2-023325 MBMS Activation procedures , from Ericsson.

[4] Tdoc S3-020532, MBMS – Trust and Threats, from Ericsson.

[5] Tdoc S3-020573, MBMS Security, from Ericsson.

[6] Tdoc S3-020533, Security protocol, from Ericsson.

[7] Tdoc S3-020534, Key Management, from Ericsson.

[8] Tdoc S3-020535, Push Re-keying, from Ericsson.

[9] [PIC] "PIC, A Pre-IKE Credential Provisioning Protocol", IETF, IPSRA Working Group, draft-ietf-ipsra-pic-06.txt, October 2002.

[10] [RFC-2284] "PPP Extensible Authentication Protocol (EAP)", IETF, RFC 2284, March 1998.

[11] IETF RFC 2617 (1999) "HTTP Authentication: Basic and Digest Access Authentication".

[12] Draft-ietf-sip-digest-aka-01: "HTTP Digest Authentication Using AKA". April, 2002.

[13] 1889 RTP: A Transport Protocol for Real-Time Applications. Audio-VideoTransport Working Group, H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson. January 1996. (Format: TXT=188544 bytes) (Status: PROPOSED STANDARD)

[14] [SRTP] http://www.ietf.org/internet-drafts/draft-ietf-avt-srtp-05.txt

[15] draft-arkko-pppext-eap-aka-04, June 2002, "EAP AKA Authentication".

[16] IETF RFC 2616 “Hypertext Transfer Protocol -- HTTP/1.1”

[17] IETF RFC 3310 “ Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)”

[18] Arkko et. al. draft-ietf-msec-mikey-04.txt, September 2002

[19] D. Halevy, A. Shamir, The LSD broadcast encryption scheme, CRYPTO’02, Springer-Verlag Berlin Heidelberg, 2002

[20] D. Wallner et. al, Key management for Multicast: Issues and Architecture, IETF RFC 2627, June 1999

[21] Draft-ietf-sip-digest-aka-01: "HTTP Digest Authentication Using AKA". April, 2002.