

Agenda Item: MBMS 6.3; GAA 5.3
Source: Siemens
Title: MBMS Key distribution
Document for: Discussion

1. Introduction

For MBMS, a traffic encryption key (TEK) needs to be distributed from the BM-SC to many UE's. This distribution needs to be secured and only authorized UE's may be able to receive a TEK. This TEK distribution can be done (method-A) UE-individually using a point-to-point connection or (method-B) for a group of UE's at the same time using multicast methods. This last method requires an additional Key Hierarchy Level for KEKs to guarantee that only the intended group of UEs need to be able to decipher the TEK. SA3 needs to decide soon whether only method-A (1) will be accommodated within Rel-6, or (2) both methods-A and B. Due to its complexity it may also be possible that method-B may not be realised soon (3). So if the decision is made in favour of (1), then the extensibility of selected key distribution protocol for Rel-6 to future releases may be an important design goal. This paper explores method-A, but also takes a look at the extensibility issue. It also takes a look at how the key distribution flow may relate to the flows described within TS 23.246 [1] and to the use of an Authentication Proxy. The use of MIKEY is also analysed as key distribution protocol.

2. Key distribution discussion

2.1 Key distribution flows

Previous SA3-discussion have highlighted that *'the UE needs to be able to trigger a TEK distribution'*. Due to the mobile specific environment, the UE could have been unreachable for some time and therefore this requires that the UE recognizes TEK mismatches as well as TEK lifetime expiration.

This TEK distribution may be needed urgently in certain circumstances, so this requires a guaranteed short-delay message delivery between the UE and the BM-SC. Within the Mobile network, a PDP context need to be set-up by the UE towards the GGSN that can reach the selected BM-SC. The BM-SC is not able to set-up a PDP context to a selected UE, so therefore for method-A the UE shall be able to trigger the TEK distribution after reserving the necessary routing resources within the mobile core and radio network. This would suggest following key

distribution flow.

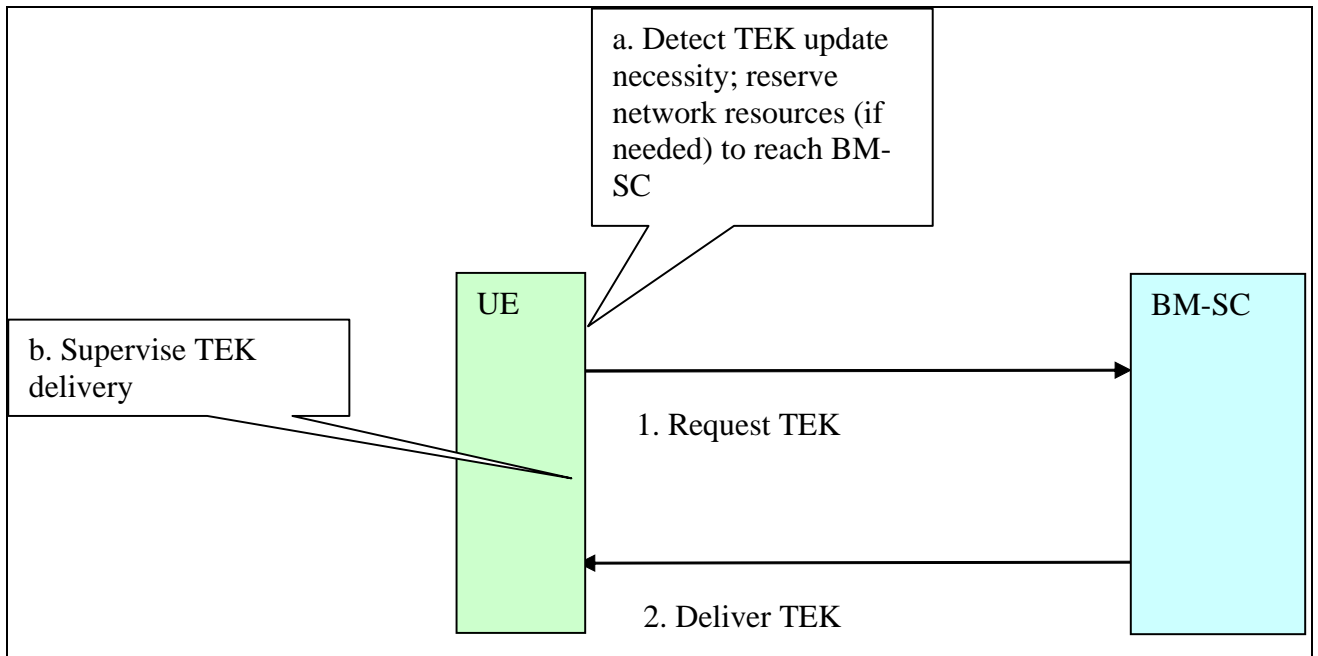


Figure 1: Simplified key distribution flow

State-a in figure 1 may be triggered by various events e.g. The BM-SC could have sent a TEK update message on some broadcast channel or the UE detected that the TEK lifetime is about to expire. While the UE has to supervise the key delivery in any case, there is no strong necessity for having a reliable transport channel between the UE and the BM-SC. The use of UDP might be favourable over TCP transport while the latter requires extra handshake messages, and so adds load to the network and adds delays to the key delivery. Bursts of TEK requests can be smoothed by implementing random timers on the UE. The decision to go over TCP versus UDP may affect the selection of the possible application layer protocols for key distribution. A TEK request message over http would be out of scope if UDP is favoured.

Ericsson have already several times proposed to use MIKEY for TEK distribution. The flow¹ that was suggested in the Ericsson papers [3] was basically similar with figure 1. Figure 2 contains the details from [2] section 3.1 .

¹ Message flow based on the existence of a pre-shared secret in BM-SC and UE. This pre-shared secret can be delivered by the GAA to both entities before the TEK distribution. (see section 2.4)

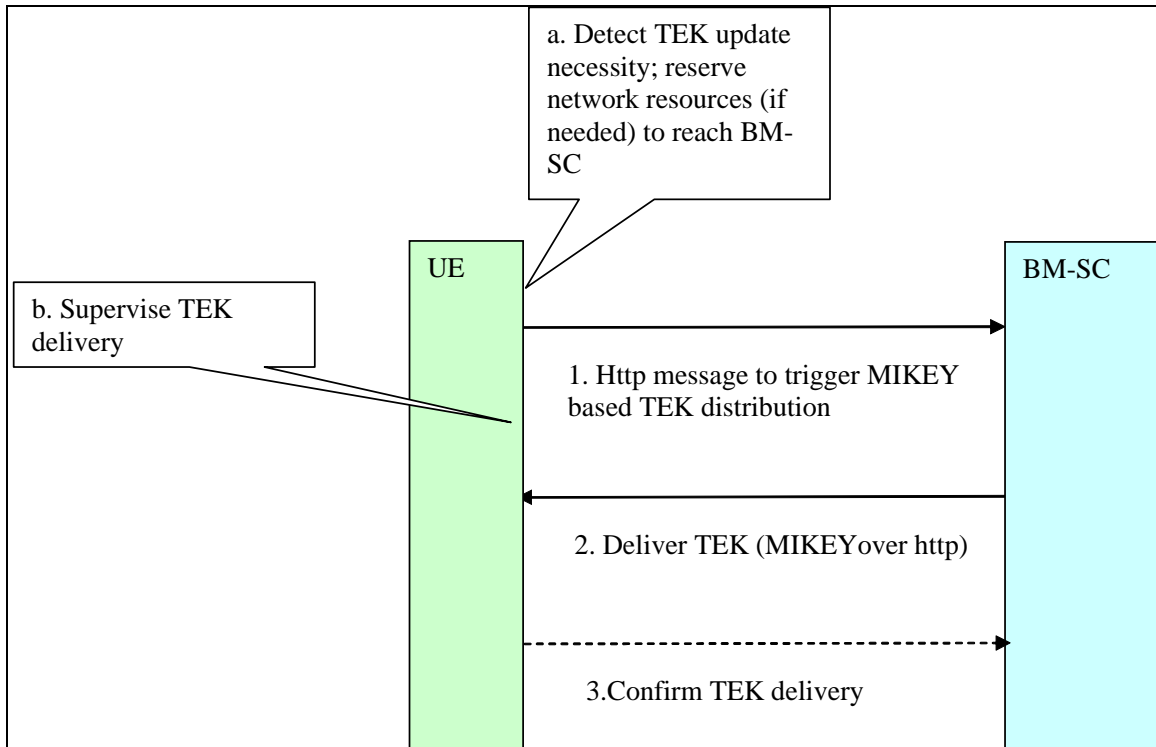


Figure 2: Use of MIKEY for key delivery [3]

Message 1 is not a MIKEY message. The use of http is taken as an example from [3] but other protocols could be used as well, as long as it delivers the necessary data to the BM-SC to be able to deliver the right TEK to the UE.

Message 2 and 3 can be detailed as follows (from Section 3.1 of [2])

Message 2 (MIKEY I_MESSAGE) = HDR, T, RAND, [IDi], {SP}, KEMAC

Where the TEK is contained within KEMAC, encrypted and authenticated, T is a time-stamp, IDi is the BM-SC identification.

Message 3 (MIKEY R_MESSAGE)= HDR, T, [IDr], V

The responder message 3 is optional, and serves to obtain mutual authentication [2]. When the UE is assigned to have the TEK retrieval responsibility, then it also can be argued that the R_MESSAGE is not really necessary. If message 2 does not arrive on time then the UE has to reinitiate the retrieval. The key delivery can be handled completely stateless at the BM-SC when leaving out message 3.

From this detailed flow it becomes also clear that MIKEY has been designed to be initiated by the BM-SC (serving as TEK distributor), therefore an out of band message (with respect to MIKEY) is needed to be able to trigger the TEK delivery. This message 1 needs to carry the right information to be able to select the right pre-shared key (e.g. UE-identity, BM-SC service id, pre-shared secret id) at the BM-SC. The UE has to assure that the pre-shared secret (KEK) is in place before the delivery of TEK is started, but it may still happen that the key KEK is not in place at the required time (e.g. due to BSF or HSS unavailability), so message 2 needs to be able to transport error causes, or the UE simply repeats message 1 a specified number of times.

2.2 The use of an Authentication Proxy for MBMS

In [4] Ericsson suggested to use client authentication via an http authentication proxy (AP) whereas the MIKEY protocol is used to carry the TEK. MIKEY also has the capabilities to provide authentication between the UE and BM-SC, but this feature of MIKEY was not used in [4]. In addition, the MIKEY capabilities to encrypt the key were not used, rather encryption was assumed to be provided by hop-by-hop tunnels between UE and AP, and between AP and BM-SC. But this may be desirable, in later 3GPP releases, to have end-to-end security between UE and BM-SC, e.g. for the purposes of UICC support (see below). If AP and MIKEY key distribution encryption/authentication were used, this would require two pre-shared secrets to be installed (one between UE and BM-SC, and one between the UE and the AP).

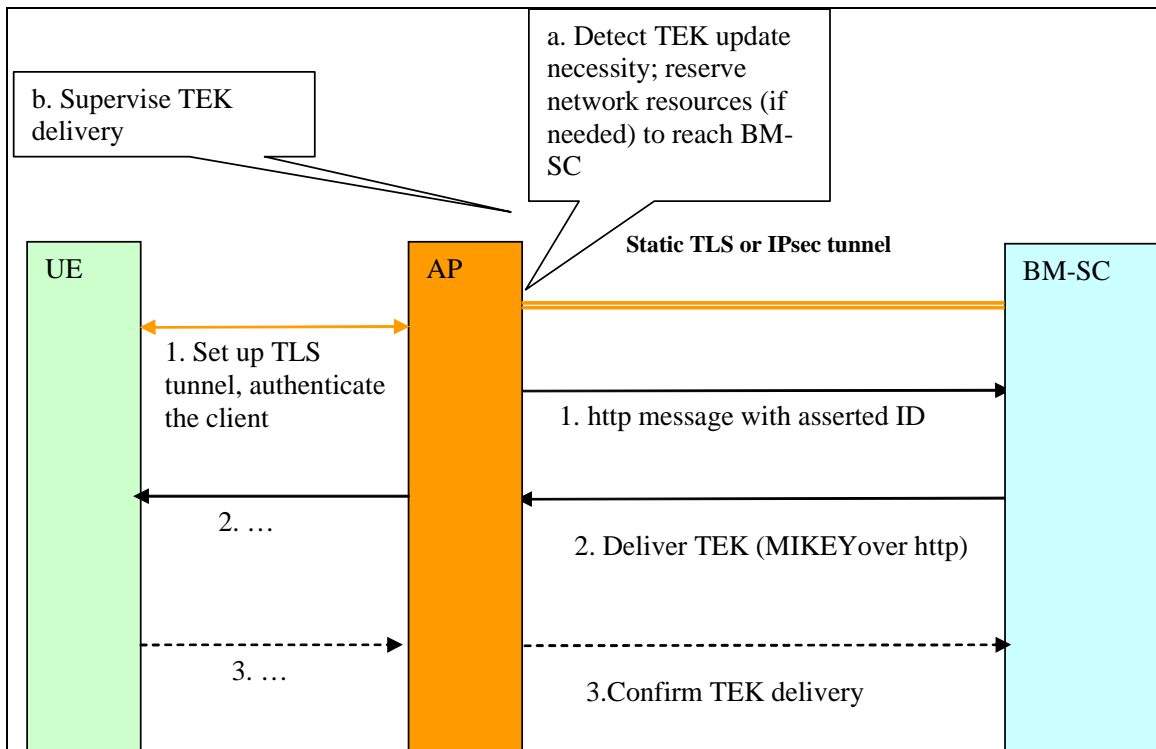


Figure 3: The use of an Authentication Proxy

Using the pre-shared secrets (KEK) directly between the BM-SC and the UE, avoids setting up a TLS tunnel to the AP. The disadvantage that an AP can read out the KEK, goes away. In addition, there is no need for a TLS tunnel when all authentication and encryption is done at the key distribution protocol itself. The necessity for setting up a TLS-tunnel for each ptp key distribution was criticized at SA3#29. The availability of https-stack can be expected in Rel-6 terminals due to the presence-feature, but NOT the availability of a TLS tunnel to the AP at the time of TEK delivery, as the management of data on the presence server by the user is a relatively rare event, so that even when a user is using presence, one cannot assume that a TLS tunnel is in place for reuse in MBMS.

The TLS stack is expected to be implemented within the ME as it has to be shared by other access

towards the AP. Consequently the TEK drops out at the ME. **Such a solution based on AP is therefore not extensible towards UICC based MBMS applications in future.** When making a decision for MBMS, SA3 has to consider the consequences of this decision.

2.3 Possible optimizations to MIKEY based key distribution.

The analysis in section 2.2 suggests solutions with encryption and authentication provided by the key distribution protocol itself. Message 1 and 2 of figure 2 could also be optimized i.e. the MIKEY draft could be adapted for MBMS as alternative to the use of http/TLS to trigger the TEK delivery.

Message 1 and messages 2 of figure 1 would then translate into²:

Message 1 (MIKEY I_MESSAGE) = HDR, T, IDi, Key-Ref, V

Where the V is a MAC on the previous data based on the pre-shared key (that is derived from the GAA/BSF). IDi and Key-Ref are needed for the BM-SC to look up the right pre-shared key.

Message 2 (MIKEY R_MESSAGE)= HDR, T, IDr, {SP}, [Error Code], KEMAC

Where the TEK is contained within KEMAC, encrypted and authenticated, T is a time-stamp, IDr is the BM-SC identification.

Within the above flow the client authentication takes place a MIKEY level and not at http level as suggested by [4].

2.4 Installation of the pre-shared secret (KEK) before running the TEK distribution.

Section 8.2 of [2] Stage-2 MBMS specification specifies a MBMS service activation flow that requires a PDP context to the BM-SC.

² This is roughly sketched. Other fields or changes might be required.

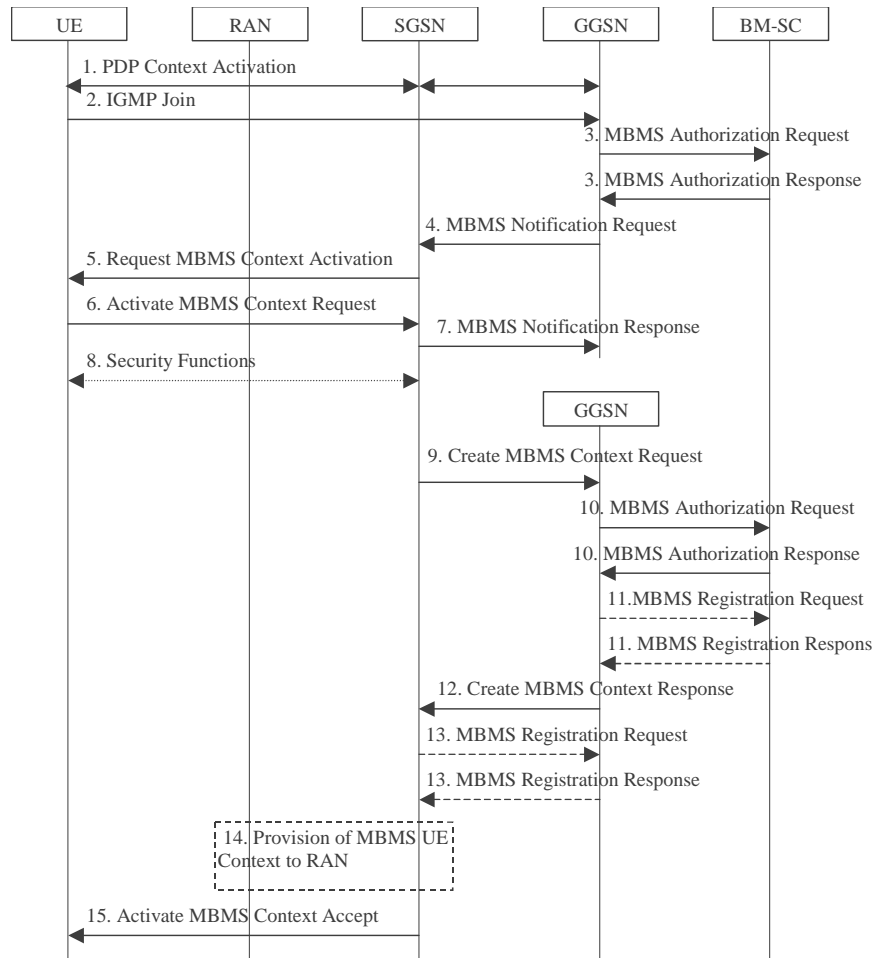


Figure 4. The activation of an MBMS multicast service

The first TEK distribution could be attached to that flow in order to take advantage of an available PDP context towards the BM-SC.

Within Figure 5 a possible flow is drafted. The detailed procedures will depend on the GAA-discussion.

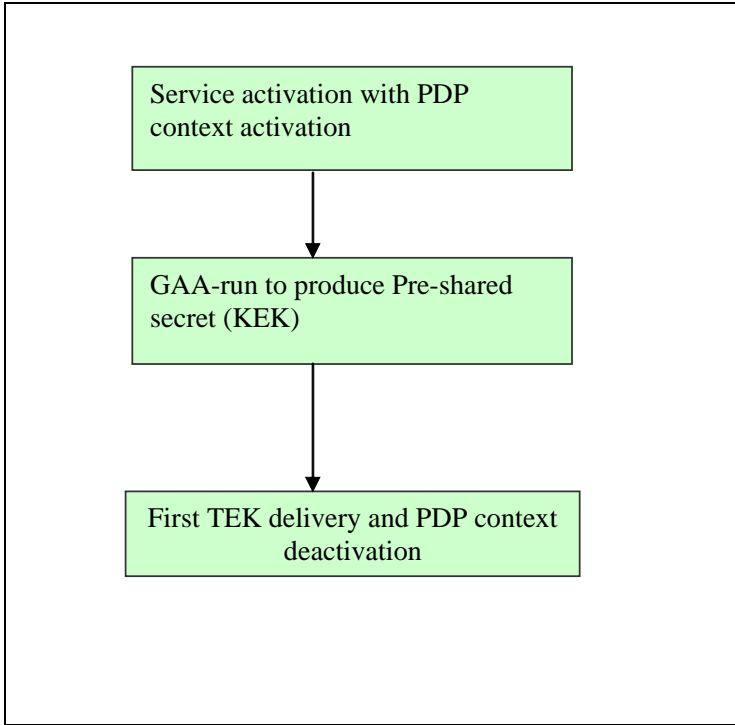


Figure 5: First TEK delivery attached to the Service activation

3. Conclusions

This paper raised following questions that need be answered before selecting a TEK distribution protocol.

- Key distribution type (Ptp or Ptm):
 - Would it be preferable to use the same TEK distribution protocol for method-A³ and B⁴ ?
 - Will both methods A and B be realized within Rel-6 ?
 - Will method B be realized soon after Rel-6 or not at all ?
- Is it acceptable to transport the TEK via an unreliable delivery protocol (e.g. UDP) as the UE has to supervise the delivery anyhow for point to point delivery ?

This paper also highlighted various open issues with respect to the use of an AP and MIKEY for use in MBMS:

- Is extra IETF work required for transporting MIKEY over http or UDP ? (The draft rfc [2] suggest only that MIKEY can be tunneled into SIP and RTSP).
- Can MIKEY be further optimized for use in MBMS as suggested by section 2.3 ?
- Does SA3 want to keep open the possibility to extend the selected TEK distribution protocol to a UICC based TEK delivery ? If so, a more detailed study is needed before accepting a concrete protocol proposal. The used GAA-solution shall not be in contradiction with it.

Siemens proposes to study the above items in more detail, to be able to take a decision at SA3#31.

4. References

- [1] S3-033207: 3GPP TS 23.246 V2.0.0 (2003-09): Broadcast/Multicast Service (MBMS); Architecture and Functional Description; *Version to be presented for approval at SA#21, September 2003*
- [2] draft-ietf-msec-mikey-07.txt: MIKEY: Multimedia Internet KEYing Internet Engineering INTERNET-DRAFT Expires: December 2003
- [3] S3-030368: Introducing SRTP and MIKEY in TS 33.246, Ericsson, SA3#29, San Francisco, July 2003
- [4] S3-030367: Access to Application Servers using HTTP in MBMS, Ericsson, SA3#29, San Francisco, July 2003

³ Point to point key distribution.

⁴ Point to multipoint key distribution