3GPP TSG SA WG3 Security — S3#33 **S3-040234**
10 - 14 May 2004
Beijing, China

Agenda Item: MBMS
Source: Ericsson, Nokia

Title: MBMS key management with MIKEY

Document for: Discussion /Decision

1. Introduction

MIKEY [1] has been proposed earlier for MBMS key management, e.g. in SA3#32 in [2] and [3].

This contribution discusses the suitability of MIKEY for MBMS key management.

2. Discussion

2.1 Status of MIKEY in IETF

MIKEY protocol has been approved by IESG and it is in RFC editor queue waiting to be published. The document includes also a MIME type definition for MIKEY. Thus it can be carried, e.g. over HTTP.

2.2 Need to enhance MIKEY due to MBMS requirements

In meeting #32 SA3 decided to adopt a two-tiered keying mechanism for MBMS. Since the MIKEY developed in IETF does not support this, MIKEY has been enhanced to support two-tiered keying and meet other MBMS specific requirements.

The enhancements to MIKEY should be specified in IETF, but due to the time constraints of Rel-6 the enhancements are specified in 3GPP and possibly later in IETF in the form of an RFC.

2.3 Features of enhanced MIKEY

The enhanced MIKEY is compatible with IETF MIKEY in the sense that if IETF MIKEY receives an enhanced MIKEY message, it will be able to gracefully reject the message without crashing and inform the sender. The enhancements have been implemented using general extension payloads to ensure compatibility. The deployment of enhanced MIKEY is more cost efficient since the standard IETF MIKEY can be turned into enhanced MIKEY with minimal implementation effort.

Enhanced MIKEY supports two-tiered keying where the MSK is sent point to point to the UE and MTK key is sent in multicast manner [4].

Enhanced MIKEY is compatible with GBA. MIKEY may use HTTP as a transport protocol for MSK delivery messages, if HTTP digest is used for user authentication in Ua interface.

Enhanced MIKEY supports both ME and UICC based key management solutions and a smooth migration from ME solution to UICC solution. This is achieved since enhanced MIKEY can take advantage of the GBA_U concept [5].

Enhanced MIKEY can support both push and pull key delivery mechanisms. MIKEY is originally a push protocol, but some other protocol such as HTTP digest can be used by the UE to trigger MSK delivery from the BM-SC to the UE.

3. Conclusion

The contribution has shown that MIKEY offers a complete solution for MBMS key management including migration from ME based solution to UICC solution.

It is proposed that the enhanced MIKEY is chosen as key management protocol for MBMS. The detailed descriptions of MIKEY in MBMS are found in companion contribution [4].

4. References

[1] MIKEY: Multimedia Internet KEYing, draft-ietf-msec-mikey-08.txt

[2] TD S3-040059, Enhanced MIKEY in MBMS, SA2#32, Ericsson

[3] TD S3-040081, MIKEY in MBMS, SA2#32, Nokia

[4] TD S3-0400xx, Extension payloads to MIKEY to support MBMS, SA3#33

[5] TD S3-040218 GBA_U: Bootstrapping secrets to the UICC, SA3#33

[6] IETF RFC 3711, The Secure Real-time Transport Protocol