3GPP TSG SA WG3 #28 **S3-030250**

6-9 May 2003

Berlin, Germany

Agenda Item: 6.21 MBMS

Source: Ericsson

Title: Status of SRTP and MIKEY in IETF

Document for: Information

1. Introduction

Secure RTP (SRTP) is an application layer security protocol, which is one candidate to be used as security protocol for streaming MBMS media. An analysis of SRTP and some other security protocols was presented in [S3-020533], which proposed SRTP to be used for streaming MBMS applications.

Multimedia Internet KEYing (MIKEY) is a key management protocol for secure multimedia sessions. It is one candidate to be used as key management protocol for MBMS. An analysis of MIKEY and some other key management protocols was presented in [S3-020534], which proposed MIKEY to be used for streaming MBMS applications.

Currently these protocols are being finalized in IETF (Internet Engineering Task Force). This contribution describes the standardization status of these two protocols in IETF.

2. Status of SRTP in IETF

SRTP has been developed over a relatively long time period in IETF Audio/Video Transport (AVT) Working Group. In the IETF standards track process SRTP internet draft [3] is currently under IESG review, which is the last stage before IESG Last Call and RFC status. It is likely that the RFC number will be issued during 2003. This shows that SRTP is a mature protocol and possible to be deployed in MBMS from an IETF point of view.

3. Status of MIKEY in IETF

MIKEY is a key management protocol for secure multimedia sessions which has been developed in IETF Multicast Security (MSEC) Working Group. In the IETF standards track process MIKEY internet draft is currently under IESG review, which is the last stage before IESG Last Call and RFC status. It is likely that the RFC number will be issued during 2003. This shows that MIKEY is a mature protocol and possible to be deployed in MBMS from an IETF point of view.

3. Conclusion

This contribution has shared information for 3GPP SA3 WG on the current status of SRTP and MIKEY in IETF, since they are regarded as a strong candidate for security and key management protocols, respectively, for MBMS.

4. References

[1] Tdoc S3-020533, Security protocol, Ericsson

[2] Tdoc S3-020534, Key management, Ericsson

[3] The Secure Real-time Transport Protocol, draft-ietf-avt-srtp-06.txt, work in progress

[4] MIKEY: Multimedia Internet KEYing, draft-ietf-msec-mikey-06.txt, work in progress