3GPP TSG SA WG3 Security — S3#33 **S3-040228**
10 - 14 May 2004
Beijing, China

Agenda Item: MBMS
Source: Ericsson

Title: SRTP for streaming protection in MBMS

Document for: Discussion /Decision

1. Introduction

SRTP [1] is a security protocol and a profile of RTP, which can provide confidentiality, message authentication and replay protection to the RTP/RTCP traffic. SRTP can achieve high throughput and low packet expansion. SRTP protocol has been developed especially for securing streaming applications.

This contribution proposes to use SRTP for protecting streaming MBMS data.

2. Discussion

2.1 Status of SRTP in IETF

SRTP has achieved RFC status and it has RFC number 3711.

2.2 Why SRTP is suitable for MBMS

The bullet points below give reasoning why SRTP is suitable for MBMS.

1. SRTP is ready and proven security protocol that has undergone a thorough review in IETF. There is no need to develop a new protocol.

2. SRTP does not need modifications due to MBMS multicast
   SRTP is designed from the start to support also streaming multicast applications. SRTP is not in the way of multicast properties of RTP.

3. SRTP is compatible with MIKEY [2]
   SRTP is compatible with MIKEY that is a strong candidate for key management protocol for MBMS. Together with GBA and MIKEY SRTP offers a complete solution for MBMS streaming applications. It is important that chosen key management and security protocols have proven interoperability. It can be noted that SRTP does not need modifications when used with the enhanced MIKEY, see []. It should be noted that SRTP does not exclude other key management solutions. SRTP includes a field (MKI, master key identifier) where the Key-ID can be carried in the MBMS data as is described in TS 33.246 [4].

4. SRTP has integrity protection
   Together with source origin authentication (SOA) integrity protection may be useful for MBMS data, as is discussed in another paper from Ericsson [5].

5. SRTP has no possibility for selective encryption
   Thus possible threats due to selective encryption [6] are not applicable to SRTP and content privacy is not threatened.

6. Harmonization with IETF and 3GPP2
   Since SRTP is in RFC status, it is by default harmonized with IETF. SRTP has also been chosen by 3GPP2 for BCMCS service for protecting streaming data. Choosing SRTP for MBMS streaming data will harmonize the streaming protection solutions in IETF, 3GPP and 3GPP2.

3. Conclusion

The contribution has shown that SRTP is a security protocol that can be used for protecting MBMS streaming data.

It is proposed that SRTP is chosen as security protocol for MBMS streaming data, see companion pseudo CR [8].

4. References

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

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

[3] TD S3-040xxx, MBMS key management with MIKEY, SA3#33

[4] TS 33.246, Security of Multimedia Broadcast/Multicast Service, v 1.1.0

[5] TD S3-040xxx, On the need for integrity and source origin authentication in MBMS, Ericsson, SA3#33

[6] TD S3-040008, Response on protection of MBMS and DRM Streaming Services, ETSI SAGE, SA3#32

[8] TD S3-040xxx, Pseudo CR: SRTP in MBMS, Ericsson, SA3#33