3GPP TSG SA WG3 Security — S3#34 **S3-040552**

July 6 - 9, 2004

Acapulco, Mexico

Title: **SRTP for protecting of MBMS streaming data**

Source: **Ericsson**

Document for: **Discussion and decision**

Agenda Item:

Work Item: **MBMS**

1. Introduction

In SA3#33 the use of SRTP for MBMS streaming data was discussed and an LS was sent to SA4 [1] to request their guidance. SA4 has replied in LS [2] that SA4 have no technical issues with the adoption of SRTP and that SA4 believe that the final decision should be made by SA3.

SRTP [3] 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. The optional MKI and the recommended authentication tag are the only fields defined by SRTP that are not in RTPSRTP protocol has been developed especially for securing streaming applications.

This contribution proposes to choose SRTP for protecting MBMS streaming. The accompanying CR implements the changes in the TS 33.246 [4].

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 restate the reasoning from SA3#33 [5] 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.

3. SRTP is compatible with MIKEY [6]
SRTP is compatible with MIKEY that was agreed for key management protocol for MBMS in SA3#33. 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 MBMS specific extensions of MIKEY that are being developed in SA3.

4. SRTP has integrity protection
SRTP has optional support for integrity protection as is required in TS 33.246.

5. Possible support of Source Origin Authentication (SOA)
Work is under way in IETF to enhance SRTP to support SOA [7]. The work is not expected to be ready in rel-6

timeframe, but it enables to enhance MBMS streaming protection with SOA in the future releases if SRTP is chosen as the streaming security protocol.

6. SRTP has no possibility for selective encryption
   Thus possible threats due to selective encryption [8] are not applicable to SRTP and content privacy is not threatened.

7. 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

This contribution has shown that SRTP is a security protocol that is ready to be used for protecting MBMS streaming data.

It is proposed that SRTP is chosen as security protocol for MBMS streaming data. The companion pseudo CR implements the changes in the TS 33.246.

4. References

[1] TD S3-040443, LS on Protection of streaming and download MBMS, SA3#33

[2] TD S3-040461, Reply LS on MBMS security issues, SA3#34

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

[4] TS 33.246, Security of Multimedia Broadcast/Multicast Service, v 1.2.1

[5] TD S3-040228, SRTP for streaming protection in MBMS, Ericsson, SA3#33

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

[7] IETF, draft-ietf-msec-srtp-tesla-00.txt, Internet Draft, February 2004

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

3GPP TSG-SA WG3 Meeting S3#34
Acapulco, Mexico, July 6-9, 2004

Tdoc ⌘S3-040552_Att1

CR-Form-v7

CHANGE REQUEST

⌘	**33.246**	**CR**	**CRNum**	⌘**rev**	**-**	⌘	Current version:	**1.2.1**	⌘	

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ □ ME ☒ Radio Access Network □ Core Network ☒

Title:	⌘	SRTP for streaming protection of MBMS		
Source:	⌘	Ericsson		
Work item code:	⌘	MBMS	***Date:*** ⌘	29/06/2004
Category:	⌘	**C**	***Release:*** ⌘	Rel-6

Use one of the following categories:
- ***F*** *(correction)*
- ***A*** *(corresponds to a correction in an earlier release)*
- ***B*** *(addition of feature),*
- ***C*** *(functional modification of feature)*
- ***D*** *(editorial modification)*

Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	The protection of streaming MBMS data is not specified.
Summary of change:	⌘	It is proposed to use SRTP to protect streaming MBMS data
Consequences if not approved:	⌘	

Clauses affected:	⌘	2, 6.5

Other specs affected: ⌘

Y	N		
	X	Other core specifications	⌘
	X	Test specifications	
	X	O&M Specifications	

Other comments:	⌘	

2 References

The following documents contain provisions, which, through reference in this text, constitute provisions of the present document.

References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.146: "Multimedia Broadcast/Multicast Service; Stage 1".

[3] 3GPP TS 23.246: "Multimedia Broadcast/Multicast Service (MBMS); Architecture and Functional Description".

[4] 3GPP TS 33.102: "3G Security; Security Architecture".

[5] 3GPP TS 22.246 "MBMS User Services"

[6] 3GPP TS 33.220: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture".

[7] 3GPP TS 31.102: "T3-specification describing MBMS application and interface procedures on UICC"

[8] IETF RFC 2617 "HTTP Digest Authentication”

[9] IETF RFC 3711 "Secure Real-time Transport Protocol”

[10] "MIKEY: Multimedia Internet Keying”, draft-ietf-msec-mikey-08.txt”

Editor’s note: The reference to MIKEY should be updated when MIKEY receives RFC status.

****************************NEXT CHANGE****************************

6.5 Protection of the transmitted traffic

6.5.1 Protection of streaming data

6.5.1.1 Usage of SRTP

When it is required to protect MBMS streaming data SRTP (Secure Real-time Transport Protocol) as defined in [9] shall be used to protect MBMS streaming data.

The data transmitted to the UEs is protected by a symmetric key (an MTK) that is shared using extended MIKEY by the BM-SC and UEs that are accessing the MBMS service. -MTK shall be used as the master key in SRTP key derivation to derive the SRTP session keys as defined in chapter 4.3 of [9].

The protection of the data is applied by the BM-SC. In order to determine which key was used to protect the data ~~a Key_ID~~ MKI (Master Key identifier) field as defined in [9] is included with the ~~protected data~~SRTP packets. The MKI ~~Key_ID~~ will uniquely identify the MSK and ~~contain other information needed to calculate~~ the MTK. The form of MKI shall be a concatenation of MSK ID and MTK ID, i.e. MKI = (MSK ID || MTK ID).

If the SRTP packets are to be integrity protected, the SRTP authentication tag is appended to the packets as defined in [9].

SRTP security policy parameters, such as encryption algorithm, are transported in MIKEY Security Policy payload as defined in chapter 6.10.1 in [10].

6.5.1.2 Packet processing in the UE

When the SRTP module receives a packet, it will check if it has the MTK corresponding to the value in the MKI field in the cryptographic context.

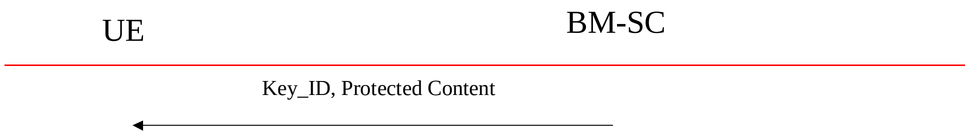
NOTE: The SRTP module does not need to interpret the MKI field semantics. It only checks whether it has the MTK corresponding to the MKI value.

If the check is successful, the SRTP module processes the packet according to the security policy.

If the SRTP module does not have the MTK, it will request for MTK corresponding to the MKI from the key management module. When the key management module returns a new MTK, SRTP module will derive new session keys from the MTK and process the packet. However, ~~If~~ if the ~~UE~~ key management module does not have the MSK indicated by ~~Key_ID~~MKI, then it should fetch the MSK using the methods discussed in the clause 6.3. The MTK is derived according to the methods described in clause 6.4.

Note: including the ~~Key_ID~~MKI with the protected data stops the UE trying to decrypt and render content for which it does not have the MSK.

The below flow shows how the protected content is delivered to the UE



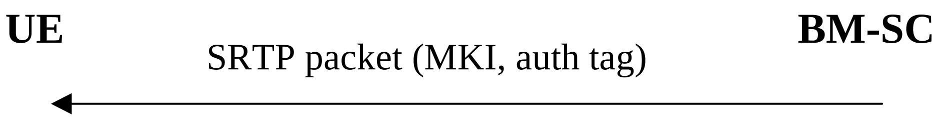


Figure x. Delivery of protected streaming content to the UE.

After using a key to decrypt protected traffic, the UE deletes any older key for this multicast service.

Editor's note: this section may contain several protection methods.

Editor's note: if SRTP is chosen, the master key identifier can be used to indicate the current MBMS key whichever key management method is chosen