3GPP TSG SA WG3 meeting #25 **S3-020533**

October 8-11, 2002

Munich, Germany

Agenda Item: 7.19 MBMS

Source: Ericsson

Title: MBMS – Security layer selection

Document for: Discussion and decision

1. Introduction

This document is written to illustrate the different options for security layer, giving input to the decision process at 3GPP. Also, a comparison table of different approaches is included together with a conclusion of results of "security layer selection" evaluation. The target for security provision is MBMS system.

Ericsson proposes that SA3 adopts the following working assumptions:

1. Protection of MBMS content shall be at application layer
2. SRTP as security protocol for securing MBMS content

1.1 Brief overview of security protocols

For multicast or broadcast transmissions, we must use connectionless protocols. This is due to the fact that as the source generates the transmission, it cannot be responsible for reliable end-to-end connection because the data may be replicated in any of the downstream "routers". Note that "multicast (push) file downloading" was not included in considerable way in this study.

Few protocols NOT SUITABLE for connectionless transfer:

In practice, this means that IETF security protocols, which only run over TCP, cannot be used for MBMS media distribution. Such connection dependent IETF security protocols are for example:

- SSL/TLS (Secure Sockets Layer/Transport Layer Security)

- Secure HTTP

- Secure Shell

Few protocols POSSIBLE for connectionless transfer:

There are few IETF security protocols, which may run over connectionless transport, such as:

- IPsec AH & ESP (with shared security association)

- SRTP (Secure Real-time Transport Protocol) [SRTP]

2. Criteria for security layer evaluation

We examined the existing requirements of 3GPP on security issues. We concluded that the decision of security layer issue for MBMS service should be based on the criteria represented in below subchapters. As a basis, we used [USP], which define objective criteria for evaluating security mechanisms within UMTS. The origin of each individual criterion is indicated in the appended reference.

2.1 Security service provision

C-S1: Home environment trust in the serving network for security functionality is minimized [PRI].

C-S2: Fitness for purpose [USP]

C-S3: Security proof [USP]

C-S4: Possibility to protect user against active attacks [PRI]. (In active attacks, equipment is used to impersonate parts of the network to actively cause lapses in security.)

C-S5: Algorithm maturity and exposure [USP].

C-S6: Availability of similar replacements [USP].

2.2 Communications overheads

C-C1: Minimizing the number of messages [USP].

C-C2: Minimizing total length of messages [USP].

C-C3: Minimized message expansion (e.g. padding in block ciphers) [USP].

C-C4: Performance effects (e.g. minimize the effects of bit errors) [USP].

2.3 Administration overheads

C-A1: The operation of security features is independent of the user, i.e. the user does not have to do anything for the security features to be in operation [PRI]. However, greater user visibility of the operation of security features will be provided to the user.

C-A2: The user may want increased control over his service profile, which he might manage over the Internet, and over the capabilities of terminal. It will be possible to download new services and functions using systems such as MExE and SIM Application Toolkit [PRI].

C-A3: Minimized key storage (may have very significant advantages) [USP].

C-A4: Minimized storage of other security parameters: (e.g. some authentication mechanisms require all "recently received" messages to be stored to detect malicious replays occurring within the tolerance interval for synchronized clocks.) [USP].

C-A5: Minimized need for trusted third parties: (e.g. authentication mechanism may require an on-line authentication server, an off-line certification authority or an on-line trusted time server to provide clock synchronization) [USP].

C-A6: Minimized involvement of other entities (also the necessary level of trust in such entities should also be minimized) [USP].

C-A7: System should work without any reduction in security when a user roams [USP].

2.4 Processing and other hardware overheads

C-P1: The terminal will be used as a platform for e-commerce and other applications [PRI]. Multi-application smart cards where the USIM is one application among many can be used with the terminal. The smart card and terminal will support environments such as Java to allow this.

C-P2: Cryptographic algorithm calculation (minimized complexity) [USP].

C-P3: Minimized other computation [USP].

C-P4: Limited special hardware needs: (e.g. minimized HW requirements to generate random values or unpredictable pseudo-random numbers) [USP].

C-P5: Matching processing requirements. Ideally, a security mechanism will match the processing requirements to the capabilities of various entities [USP].

2.5 Adherence to international standards and national regulations

C-AS0: (Not included) ISO/IEC SC27 Mechanism Standards [USP] (we assume this is not a valid requirement any more).

C-AS1: MBMS shall be interoperable with IETF IP multicast [MBMS].

C-AS2: Lawful interception (LI) requires functions to be provided in some, or all of the switching or routing nodes of a telecommunications network [HIF]. Specifically, LI has to be supported in nodes implementing P-CSCF and S-CSCF functions.

2.6 Limitations on use

C-L1: Existence of patents can be a significant disadvantage [USP].

C-L2: Export restrictions: a mechanism may be subject to widespread export restrictions [USP].

3. Results of evaluation

The results are summarized in the table below:

(Legend: G= Grade: "2" good; "1" moderate; "0" bad).

CRITERIA		**Application layer security (SRTP)**		**IP level security (IPsec with AES)**		**Radio-level multicast security**	
ID	**Description**	**G**	**Notes**	**G**	**Notes**	**G**	**Notes**
C-S	**Security service provision:**	**2**		**2**		**-**	**Mechanism not specified**
C-S1	Trust to VN	2	Not required	2	Not required	0	Required
C-S2	Fitness	2	Tailored for streaming	2	Generic properties	-	Mechanism not specified
C-S3	Security	2	AES	2	AES	-	Mechanism not specified
C-S4	Active attack	2	end-to-end	2	end-to-end	1	Require protective measures
C-S5	Maturity	1	IETF draft	2	RFC, but require changes	0	Mechanism not specified
C-S6	Substitutes	-	Not checked	-	Not checked	-	Not checked
C-C	**Comm. overheads:**	**2**		**1**		**-**	**Mechanism not specified**
C-C1	Number of messages	2	Optimal in registr. Phase (MIKEY)	1	Not optimal in registr. phase (GDOI,	-	Very probably would be minimized

					GSAKMP-L)		
C-C2	Mess. Length	2	Enable IP/UDP/RTP header compr.	0	Unable to UDP/RTP header compr.	-	Very probably would be minimized
C-C3	Expansion	2	32 bit HMAC	1	96 bit HMAC + 64 bit IV in AES-counter-mode	-	Very probably would be minimized
C-C4	Performance	2	AES in counter mode	2	AES in counter mode	-	Very probably would be optimized
C-A	**Adm. Overheads:**	**2**		**1**		**1**	
C-A1:	Ease of use	1	May require installation	2	Transparent to user	2	Simple
C-A2:	Incr. Control	2	Flexible user interface	1	Problematic user interface	1	Limited user interface
C-A3:	Key storage	2	Minimized	1	Public keys for registration and re-key	-	Very probably would be minimized
C-A4:	Other params.	2	Limited	1	ESP params, IV	-	Very probably would be minimized
C-A5:	3rd parties	1	Loose clock accuracy needed	0	PKI for GDOI, GSAKMP-L	1	Visited network
C-A6:	Other entities	2	Only terminal and BM-SC application	1	IP stack manufacturer	0	Involve several mobile nw nodes
C-A7:	Roaming	2	BM-SC terminated	2	BM-SC terminated	0	NW dependant crypto
C-P	**Processing & other HW overheads:**	**2**		**2**		**-**	**Mechanism not specified**
C-P1:	Multi-smart cards	-		-		-	
C-P2:	Crypto complexity	2	AES	2	AES	-	Very probably would be minimized
C-P3:	Other computation	2		2		-	Very probably would be minimized
C-P4:	HW dependent	2		2		-	Not specified
C-P5:	Matching processing	2	AES in counter mode	2	AES in counter mode	-	Very probably would be matching

C-AS	**Adherence to standards and regulations**	**2**		**2**		**0**	**Mechanism not specified**
C-AS1:	IP multicast	2	Possible	2	Possible	0	Network dependent multicast
C-AS2:	Lawful Interception	1	Small addition to GGSN	1	Small addition to GGSN	2	No changes needed
C-L	**Limitations**	**2**		**2**		**-**	**Mechanism not specified**
C-L1:	Patents	2		2		-	Mechanism not specified
C-L2:	Export restrictions	2		2		-	Mechanism not specified

Table 1. Summary of evaluation results

4. Conclusions

A security protocol, which operates on application layer, should be selected as the working assumption for MBMS data protection. It should be understood that any of the "0" results in table 1 may be fatal, which mean that the implementation of such approach has no rationale in terms of cost or negative deployment effects. A summary of *non-fulfilled* (received one or more "0" grades) criteria is collected in a below table:

Criteria	**SRTP**	**IPsec**	**Radio-level multicast security**
Security service provision			**Requires full trust to VN + mc security not developed**
Comm. overheads		**Full header compression not possible for long e2e (RTP) headers**	
Adm. Overheads		**PKI required for registration and re-keying**	**Involve several mobile nw nodes + serious implications to roaming**
Adherence to standards and regulations			**Standard not developed + not compatible with IETF IP multicast**

Table 2. Summary of non-fulfilled criteria

It is visible from the analysis that IP level security protocols (IPsec AH, ESP) cannot fulfil the evaluation criteria to necessary extent. However, a clear advantage of IPsec is its common usage (though, not in multicast scenarios). We also see that radio-level multicast security has difficulties or drawbacks for MBMS data security, and most importantly, it has not yet been developed. Also, the radio-level multicast security is not useful if other access than UMTS is used.

On the other hand, several application layer protocols may fulfil most of the evaluation criteria. For interoperability reasons, Ericsson suggests that the selected protocol should be (as a working assumption):

-SRTP (for streaming applications)

Secure RTP (SRTP) is an application layer protocol, which has been developed over a relatively long time period in IETF Audio/Video Transport (AVT) Working Group. Also SRTP implementations exist. More information about SRTP can be found from [SRTP], which is currently on AVT WG last call. The characteristics of SRTP are, for example: secure for unicast and multicast RTP applications; high throughput and low packet expansion; protection for heterogeneous environments (e.g. an additive stream cipher and an implicit index for sequencing/synchronization based on the RTP sequence number).

5. References

[HIF] 3GPP TS 33.108 (V5.0.0), 3G Security; Handover Interface for Lawful Interception (Release 5), 2002-06

[MBMS] 3GPP TR 23.846 (V1.1.1), Multimedia Broadcast/Multicast Service; Architecture and Functional Description (Release 6), 2002-07

[PRI] 3GPP TS 33.120 (V4.0.0), 3G security; Security principles and objectives (Release 4), 2001-03

[SRTP] http://www.ietf.org/internet-drafts/draft-ietf-avt-srtp-05.txt

[USP] UMTS 33.20 V3.1.0, (UMTS); Security Principles, 1999-02