**3GPP TSG SA WG3 Security — S3#26** **S3-020652**

**19 – 22 November 2002**

**Oxford, UK**

**Source:** **Nokia**

**Title:** **MBMS security**

**Document for:** **Discussion**

**Agenda Item:** **7.19**

## 1. BACKGROUND

Alcatel presented MBMS security discussion paper [1] in SA3#24 Helsinki meeting. This paper gave an overview of possible scenarios for protecting the MBMS traffic. It also identified various options for the level at which encryption and integrity protection should be done (application level or radio part), the entity that should be responsible for key management and the way membership management and key distribution should be done.

After this there were several contributions presented in SA3#25 Munich meeting for supporting either application or network level (i.e. radio part) alternatives. The purpose of this paper is to highlight several issues that have been found during the analysis of these alternatives.

## 2. DISCUSSION

### 2.1 Key delivery

Key delivery needs to be performed for both alternatives, but this is a more extensive problem for application level alternative than for network level one, where Rel99 procedures already exist. The choice of key delivery solution for application layer alternative can be categorized in between some 3GPP - specific solution, adaptation of 3GPP2 model, some OMA solution or IETF - specific solution.

### 2.2 Compatibility with Rel99 security for simultaneous non-MBMS services

MBMS Stage-1 specification [2] states the following:

“Dependent on terminal capabilities, it shall be possible for the user to participate in other services, while simultaneously participating in MBMS services. For example the user can originate or receive a call or send and receive messages whilst receiving advertisements”

When analyzing the application and network level alternatives, the scenario where the user simultaneously receives non-MBMS services needs to be taken into account. For network level security this implies that the feasibility of simultaneous MBMS service specific ciphering and Rel99 ciphering needs to be studied. For application layer security this means that the feasibility for disabling the network level ciphering for MBMS bearer while the Rel99 ciphering is still used for some other bearer needs to be studied.

### 2.3 Issues in introducing application level ciphering for MBMS

With application layer ciphering the application must take care of all security issues such as prevention of key copying, key delivery/synchronization and encryption. For these tasks application layer security must not require lower layer assistance other than the services already offered to the application layer in Rel99.

A general-purpose application development environment for mobile software (e.g. Java) might not be very suitable for implementing decryption. In order to allow the use of service-independent MBMS security software at the application layer, a common security solution for all MBMS applications is needed, instead of one specific for each application. This requires that a common framework for application level security needs to be specified either by 3GPP or by some external organization. The use of some external organization (OMA, IETF) is probably not feasible within Rel 6 time frame. On the other hand, 3GPP is not seen as the appropriate forum to do this work either.

### 2.4 Key management in SGSN

In network level solution SGSN should be able to advise RNC that which multicast sending this relates. SGSN sees keys but not the actual service content. Even though in case of application level solution, SGSN should know what content is coming and where it is sent to.

### 2.5 Bearer knowledge about content and stream mapping

SGSN and RNC elements have a significant role in MBMS service. SGSN has MBMS service specific contexts and two GTP tunnels (RAN-SGSN and SGSN-GGSN). GGSN for one's part does have an interface with BM-SC.

SGSN knows if it is a PDP or MBMS context in question. Additionally SGSN can figure out from the MBMS context that it's indeed a MBMS service and it knows the IP Multicast address. SGSN establishes tunnels and RNC decides which kind of mechanism it uses (p-2-m or p-2-p). However, SGSN does not know the actual packet contents when it forwards those from one GTP tunnel to another.

### 2.6 UE processing requirements and power consumption

For application level security, the possibilities for optimizing the decryption performance in the UE are more limited than when using network level security, where the optimization methods already developed for Rel99 ciphering can be more readily reused. This has to be taken into account when estimating the throughput and the power consumption of each solution.

## 3. CONCLUSION

It is proposed that SA3 takes these issues into consideration when developing MBMS security solution.

## 4. REFERENCES

[1] S3-020363 MBMS security discussion paper in SA3#24 Helsinki, Alcatel

[2] 3GPP TS 22.146 “Multimedia Broadcast/Multicast Service; Stage 1”