3GPP TSG SA WG3 Security — MBMS ad-hoc **S3z030021**
3-4 September 2003
Antwerp, Belgium

Agenda item: MBMS Security

Source: Gemplus, Oberthur, Qualcomm Europe, SchlumbergerSema,

Title: Progress report on MBMS 3GPP2 solution

Document for: Discussion and Decision

Abstract

This input paper aims at providing a progress report on the MBMS 3GPP2 framework for MBMS security.

1 Introduction

At SA3#29 meeting Qualcomm presented contributions describing the MBMS 3GPP2 security framework [1] and the BCMCS security framework [2]. The main advantages of the MBMS 3GPP2 solution compared to the others consist in avoiding threats due to valid subscribers interested in circumventing the security, reducing signalling traffic and helping harmonization process between 3GPP and 3GPP2.

This contribution gives an overview of the new studies and solutions proposed to complete the 3GPP2 solution, it answers open questions identified during previous MBMS discussions.

2 Discussion

The new proposals are addressing the following topics:

Stage 3

To answer Stage 3 needs, smart cards manufacturers have started investigations on USIM enhancement to support the MBMS key Management scheme corresponding to the 3GPP2 solution. A contribution already exists [3], which defines APDU commands for the 3GPP2 key management and proposes additional mechanisms, e.g. to address charging issues.

This contribution was discussed at T3#28 August meeting and T3 decided to send a LS to SA3 [4] with the following action for SA3:

“ T3 asks SA3 to consider the attached contribution in their discussions and to quickly inform T3 and SA1 of their decision for the MBMS key management scheme and its potential impact on the USIM specifications”

Moreover, Stage 3 studies related to the “handset-network” protocol have been performed. Cf “Integration of the key management with underlying protocol” chapter and contribution [5].

So, the Stage 3 corresponding to the 3GPP2 solution is in progress.

Integration of the key management with underlying protocol

A question raised during SA3 meeting was the integration of the key management with the underlying protocol. Some different approaches have been identified and proposed in “Integrating Key Management with the Underlying Protocol” contribution, SA3 MBMS ad-hoc, Antwerp, [5].

Re-keying

There are discussions concerning the different methods to distribute the key used to decrypt the multicast content: point-to-multipoint or point-to-point re-keying? An element of comparison between the two solutions is the estimation of the signalling overhead in delivering keys in a point-to-point manner. This study is provided in the “Updating Encryption Keys for MBMS” contribution [5], SA3 MBMS ad-hoc, Antwerp, meeting.

TS enhancement

To enhance the TS document and include the MBMS 3GPP2 solution, a pseudo CR to TS 33.246 is available [7], it provides the 3GPP2 key management description and identifies some new threats.

3 Conclusion

The MBMS 3GPP2 framework is a complete solution that addresses MBMS topic and answers new security threats associated to valid subscribers. So, we propose to approve the pseudo CR to TS 33.246 to adopt the 3GPP2 solution for MBMS.

4 References

[1] MBMS Security Framework, Qualcomm Europe, S3-030356.

[2] Presentation slides: BCMCS Security Framework, Qualcomm, S3-030451.

[3] USIM Enhancements for MBMS Support, SchlumbergerSema, T3-030599.

[4] LS from T3 on “potential USIM impact of the MBMS security framework”, T3-030696.

[5] Integrating Key Management with the Underlying Protocol, contribution to SA3 MBMS ad-hoc, Antwerp.

[6] Updating Encryption Keys for MBMS, contribution to SA3 MBMS ad-hoc, Antwerp.

[7] CR to 33.246, contribution to SA3 MBMS ad-hoc, Antwerp.