3GPP TSG SA WG3 Security — S3#30 **S3-030528**
06 - 10 October 2003,
Povoa de Varzim, Portugal

Agenda item: MBMS Security

Source: BT, Gemplus, Oberthur, QUALCOMM, SchlumbergerSema...

Title: Progress report on MBMS 3GPP2 solution

Document for: Discussion and Decision

Abstract

This input provides a continued update about the status of the 3GPP2 proposal for MBMS security, and a summary of the advantages of this solution.

Discussion

This paper aims to provide a brief update of the advantages and status of the 3GPP2 security framework, as proposed by numerous companies in [6] to provide key management for MBMS security. The underlying principle of the solution is that a long-term key BAK is stored on the UICC of subscribers, and this key is combined with broadcast seeds SK_RAND to produce short term keys SK which are used to encrypt/decrypt MBMS traffic.

This approach offers several advantages for MBMS security

- It is a generic key management solution: the keys are not tied to one underlying security protocol.
- Nevertheless, it can be easily integrated, for example, with SRTP if this is desired
- It has been noted that the Master Key Indicator field in SRTP is a natural channel for delivering SK_RAND, if SRTP is preferred [9]. (Hence the reliability of the transport of SK_RAND is inherited immediately by the Error Correction on the channel.) More generally, there is a recent contribution from Philips in RAN2 to study efficient broadcast of security-related data [11].
- It was agreed at the Antwerp ad-hoc that frequent re-keying is required because of the threat that subscribers may distribute keys [6], [12]. This UICC-based approach to generating keys allows for very frequent key updates in such a way that short-term keys are not predictable. Keys distributed with alternative ‘point-to-point’ approaches, which store keys directly on the Mobile Equipment, cannot be updated frequently without imposing an unacceptable burden on radio resources [10].
- It offers harmonization between 3GPP and 3GPP2,
- It deals naturally with roaming from home to visited BMSC

- It ties keys to a subscriber and deals naturally with the issues of subscribers USIM-roaming: it eliminates threats that subscribers may download MBMS keys to multiple devices with the same USIM.
- It proposes using existing 3GPP standards for BAK management, namely secure OTA techniques described in [5],[17]. This approach to MBMS Key Management allows further flexibility for operators to un-subscribe specific users, charge (or monitor) usage, measure quality of service, etc. The work to define the APDU commands required to support this MBMS key management functionality has begun in [4].
- It notes that 3GPP OTA remote applet management may be used to deal with upgrades of pre-Rel-6 USIMs (to make them MBMS-capable) [17].

Conclusion

The 3GPP2 framework for Broadcast-Multicast offers an efficient and standards-based key management solution designed to deal with the challenges of the trust model inherent in MBMS. Deploying the highest tier of key to a UICC offers operators considerable flexibility to manage crypto-periods and other subscription-related data.

References

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

[2] 3GPP TR 23.846: " Multimedia Broadcast/Multicast Service; Architecture and Functional Description".

[3] 3GPP TS 33.246, Technical Specification Group Services and System Aspects; Security; Security of Multimedia Broadcast/Multicast Service;

[4] USIM Enhancements for MBMS Support, S3z030009.

[5] 3GPP TS 31.115: " Secured packet structure for (U)SIM Toolkit applications ".

[6] S3z030007 Pseudo-CR to 33.246: MBMS Security Architecture.

[7] 3GPP TS 31.111: "USIM Application Toolkit (USAT)".

[8] S3z030021, MBMS_3GPP2 Progress report, Antwerp

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

[10] S3z030022, Updating Encryption Keys for MBMS, Antwerp.

[11] R20301736, Implications of key management schemes on the radio interface, Philips.

[12] Draft report of Antwerp ad-hoc.

[13] S3z030027 Introducing MIKEY in TS 33.246

[14] 3GPP TS 31.116: “Remote APDU Structure for (U)SIM Toolkit applications”

[15] 3GPP TS 31.102. Characteristics of the USIM Application

[16] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS)".

[17] Over the Air Technology, Gemplus et al, contribution to SA3#30.