3GPP TSG SA WG3 Security — SA3#33 **S3-040222**
10-14 May 2004
Beijing, China

Source: **Siemens, Nokia , Ericsson**

Title: **MBMS: Key distribution architectures analysis**

Document for: **Discussion and decision**

Agenda Item: **MBMS**

1 Introduction

At the SA3#32 two key distribution architectures have been proposed. An OTA-based architecture as available from document 50/51 (see also section 2.1 below) and GBA-based architecture (see also section 2.2 below). This contribution compares the architectures from a network point of view.

Please note that the descriptions and conclusion within section 2 and 3 of this paper may have to be reworked and supplied with further details once the first deadline (12/4/04) contributions, that give more information on the OTA-architecture, are available.

2 Overview of architectures and issues comparison

2.1 Proposed architectures

2.1.1 GBA-Based architecture[1]

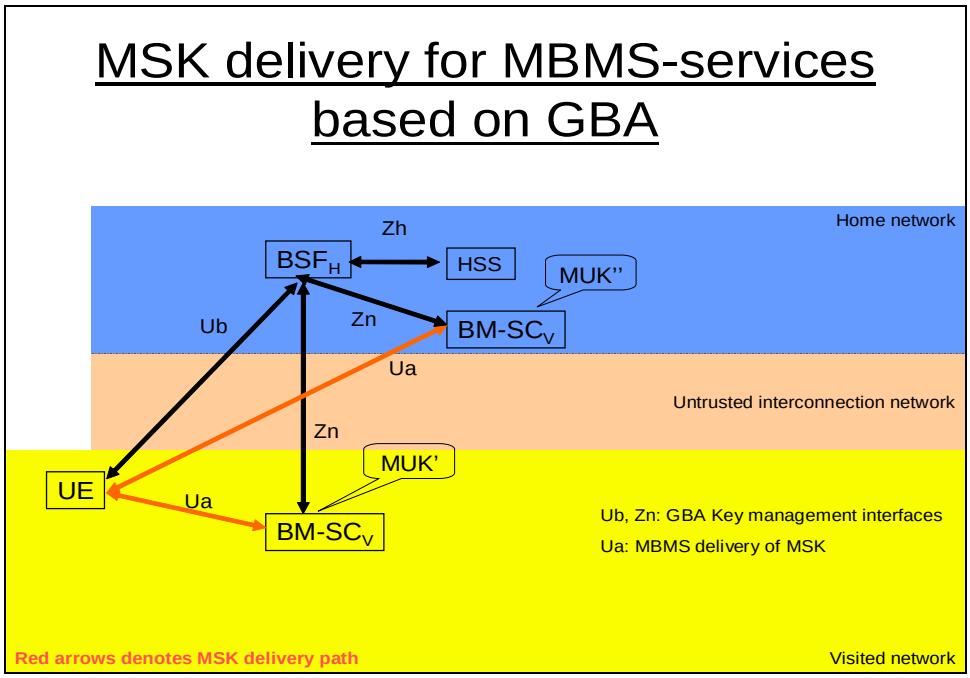

Figure 1: GBA-based MBMS key delivery in VN & HN configuration

[1] This architecture may also be given a name other then ***GBA-based architecture***. A careful reader may have noticed that the discussion topics that were brought forward in this paper are independent from GBA. As will be mentioned in section 3 in issue-2, application layer adhoc joining will be required for MBMS. In that case the BM-SC and the UE cannot rely on a pre-registration. **Therefore the OTA-architecture would also need to rely on GBA or other mechanism with similar requirements.** !

2.1.2 OTA-based architecture

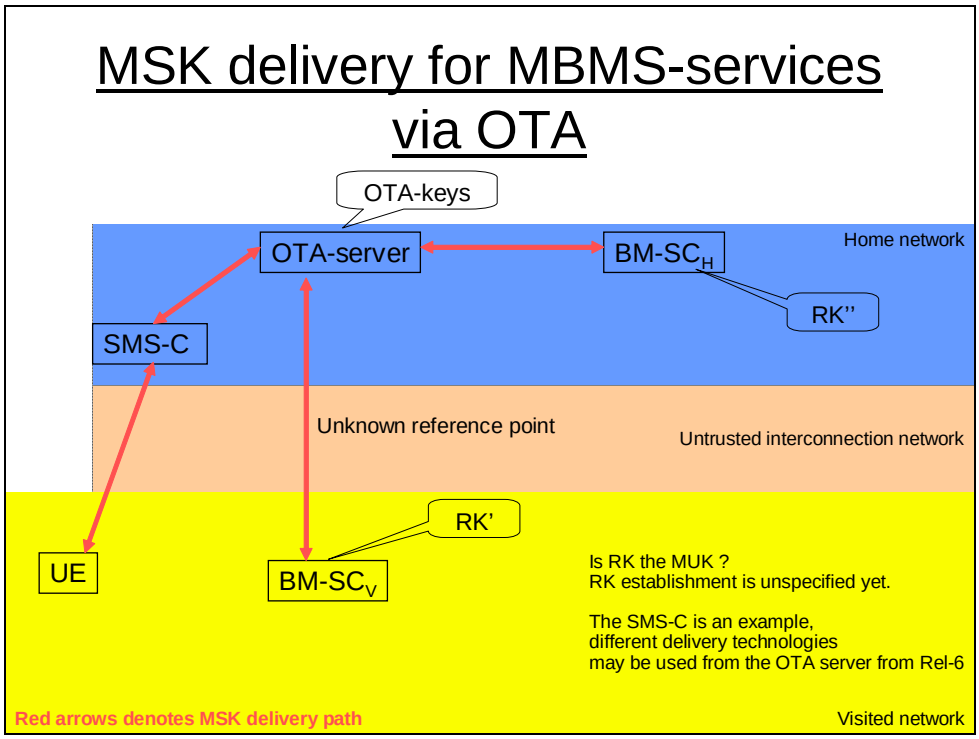

Figure 2: OTA-based MSK delivery in VN and HN Configuration

2.2 Issues of comparison

This contribution compares the architectures of section 2.1 from a network point of view on following issues.

Issue-1. Supported features

Issue-2. Efficiency in key delivery

Issue-3. Error robustness (e.g. single point of failures)

Issue-4. Load distribution

Issue-5. Extra network administration

3 Comparison

Issue-1. Supported features.

The SA3-working assumption from TS 33.246v110 section 5.1 requires that both an ME and UICC based key management solution shall be supported.

A GBA-based architecture is able to support both an ME and UICC-based key management solutions. TS 33.220 still need to be adapted to include the GBA_U concept, but early contributions (and CRs) have been made available to the SA3#33 for commenting at the first MBMS deadline of 12/4 which show that the concept has been stabilized.

An OTA based architecture is only suitable for UICC-based key management solutions.

Issue-2. Efficiency in key delivery

As already can be seen when comparing Figure 1 with Figure 2 the OTA-based delivery architecture adds an additional network component into the MSK-delivery path. Beside the preference SA3 should have for selecting architectures that are as simple as possible, the OTA based architecture works inefficient in Visited Network MBMS configurations. Although one can give arguments that this usecase will only happen for the minority of the MSK deliveries, it may still be commercially interesting to allow such usecase, especially based on adhoc application layer joining (and MSK key delivery) based concept. As to give one example, for a football game in the semi-final of the champions league between Manchester United and Real Madrid where a lot of Madrid supporters would join the VN MBMS service in Manchester (to know the status of the other ongoing semi-final) just before the start of the game. All MSK Key delivery requests originating from the BM-SC in the UK, need to go to Spain to arrive again in the UK. Furthermore the Adhoc application layer joining needs to be done in the UK.

Issue-3. Error robustness (e.g. single point of failures)

Adding an extra server (i.e. OTA server) between the sender and the recipient of the key delivery messages does not only add key delivery delays but also increases the chances for key delivery errors. The GBA-based key delivery architecture does not have this disadvantage as the BM-SC directly communicates with the UE both for the application layer joining and the MSK key delivery. The OTA-server configuration in the Home network may become a single point of failure due to issue-4.

Issue-4. Load distribution

The GBA-based MBMS key management solution adds the MSK processing load where it actually originates from (i.e. only in the BM-SC), while for an OTA-based solution also extra performance is required from the OTA-server in the Home Network. This extra load can not always be anticipated by the HN-operator when due to unknown MBMS VN-services. So this may lead to unexpected bottlenecks problems at HN, which may affect also non-MBMS OTA services.

Issue-5. Extra network administration

The BM-SC needs to know to which home network the user belongs to. Then based on HN-OTA server discovery or static addressing, the BM-SC can route the MSK message to the OTA server. For the GBA-based key delivery architecture this does not need to happen.

4 Conclusion

This paper has compared the GBA-Based key delivery architecture with the OTA-based key delivery architecture from a network point of view. It is proposed to choose the GBA-Based key delivery architecture while it is a simpler, more efficient approach for the network point of view.

5 References

S3-040050: MBMS UICC-based solution (Gemplus, Axalto, Giesecke & Devrient and Oberthur), SA3#32

S3-040051/88: Discussion paper on MBMS key management (Axalto, Gemplus, Axalto, Giesecke & Devrient and Oberthur), SA3#32

S3-040111: Comments on S3-040050/51 (Siemens, Nokia, Ericsson), SA#32