3GPP TSG SA WG3 Security — SA3#33 **S3-040345**
10-14 May 2004 reply to comments on **S3-040222**
Beijing, China

Source: **Siemens, Nokia , Ericsson (Commented by Gemplus 23/04/04)- Joint reply 3/05/2004**

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]

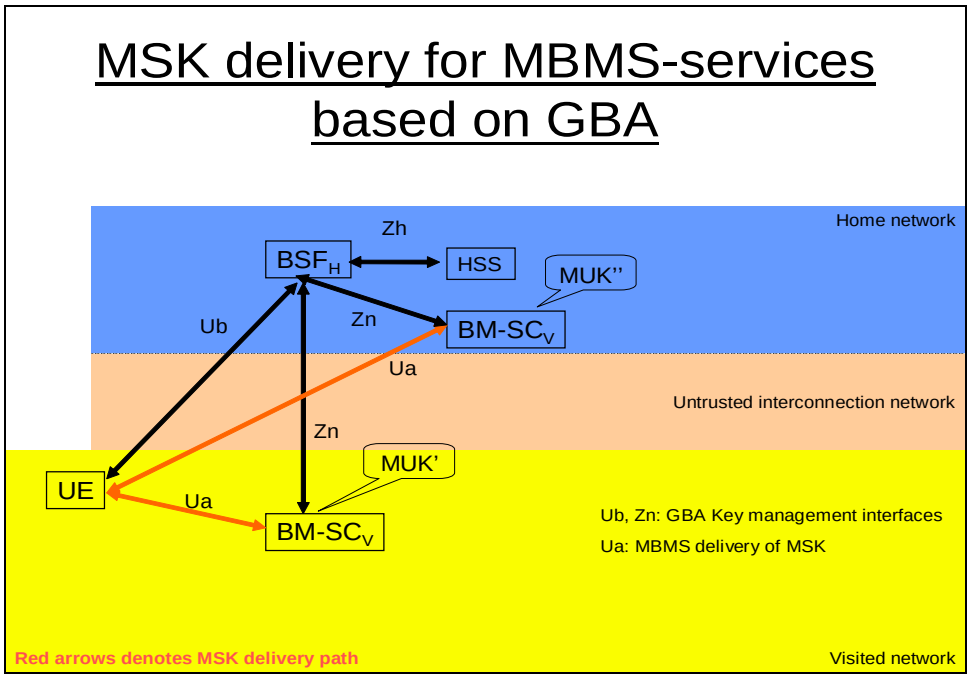

Figure 1: GBA-based MBMS key delivery in VN & HN configuration

[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

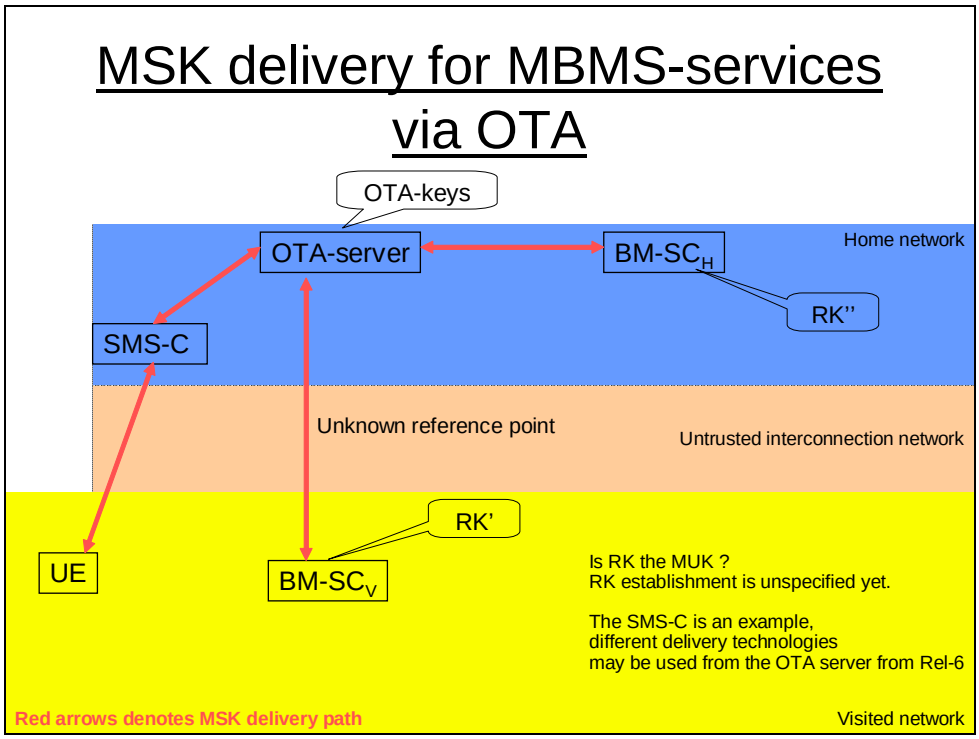

Figure 2: OTA-based MSK delivery in VN and HN Configuration

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.
<G+>
The choice between combined solution and UICC-based only solution still exists. The working assumption in section 5.1 was agreed at SA3#31 meeting and SA3 re-opened this discussion at SA3#32 meeting since several operators asked for UICC-based only solution at TSG-SA#22 meeting. The proposal for UICC-based only solution presented at SA3#32 was not rejected.
[Joint]:

The working assumption was not formally changed by SA3#32. The proposal for UICC-based only solution presented at SA3#32 was neither accepted.

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.

<G+>
With GBA, in case of new user in an Visited BM-SC, the Visited BM-SC shall contact the BSF in order to obtain a Ks_int and Ks_ext. So, extra load also affects GBA-based solution.
[Joint]:
The above statement of load distribution does not relate to the GBA-phase.
Please note that the OTA-solution also need a GBA-phase or similar functionality to support adhoc joining (without pre-installation on the card). Please also note that in case of a MSK mismatch the ME needs to send an MSK Key request to the BM-SC. How will this MSK key request be authenticated in the OTA solution? Before the load distribution of that solution can be compared with GBA, the details of that solution need to be available.

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.

<G+>
A similar issue exists for GBA. With GBA, the BM-SC also needs to know which home network the user belongs to. To receive Ks_ext_NAF or Ks_int_NAF the BM-SC shall contact the BSF which shall be placed within the Home Network according to S3-040224, so there is extra network administration in GBA for key delivery.
[Joint]:
The GBA specification already includes specification text for this, but for OTA –solution this is unknown.

<G+>

The following issue also exists:

Issue-6. Protection of UICC data

With GBA, the Visited BM-SC gains control of the smart card.
The Home Network does not longer control the data of the issued UICC, it does not know the type of modifications performed by the Visited BM-SC. Different Visited BM-SCs may compete for the same storage in the UICC MBMS containers. With OTA solution the Home Network keeps a full control of the UICC modifications even in case of roaming.

[Joint]:
As being said verbally during SA3#32 (and contribution S3-040098) both OTA, and MBMS solution based on GBA(_U) needs to take into account access control of UICC. For MBMS (and GBA_U) this means that the BM-SC should only be able to update MBMS application data and NOT other application data.

[Joint]:

The list of issues was never claimed to be exhaustive see introduction. The introduction had limited the scope to network architecture related issues. The added issue 6 does not fall under this category:
Form the network architecture point of view as an example of an additional issue we may present the following issue 7
Issue-7. Extensibility to other network architectures.

The GBA based model is designed to operate in mixed environment (with VN-access and different actors) and is more flexible to new business models where different roles might be played by different actors. This would be the case when the BM-SC would be placed outside the operator network (but which is not a working assumption for MBMS at the moment).

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